# Industrial Secure Router User's Manual

**First Edition, February 2013**

**www.moxa.com/product**

© 2013 Moxa Inc. All rights reserved.
Reproduction without permission is prohibited.

# Industrial Secure Router User's Manual

The software described in this manual is furnished under a license agreement and may be used only in accordance with the terms of that agreement.

## Copyright Notice

Copyright ©2013 Moxa Inc.
All rights reserved.
Reproduction without permission is prohibited.

## Trademarks

The MOXA logo is a registered trademark of Moxa Inc.
All other trademarks or registered marks in this manual belong to their respective manufacturers.

## Disclaimer

Information in this document is subject to change without notice and does not represent a commitment on the part of Moxa.

Moxa provides this document as is, without warranty of any kind, either expressed or implied, including, but not limited to, its particular purpose. Moxa reserves the right to make improvements and/or changes to this manual, or to the products and/or the programs described in this manual, at any time.

Information provided in this manual is intended to be accurate and reliable. However, Moxa assumes no responsibility for its use, or for any infringements on the rights of third parties that may result from its use.

This product might include unintentional technical or typographical errors. Changes are periodically made to the information herein to correct such errors, and these changes are incorporated into new editions of the publication.

## Technical Support Contact Information

**www.moxa.com/support**

**Moxa Americas**
Toll-free: 1-888-669-2872
Tel: +1-714-528-6777
Fax: +1-714-528-6778

**Moxa China (Shanghai office)**
Toll-free: 800-820-5036
Tel: +86-21-5258-9955
Fax: +86-21-5258-5505

**Moxa Europe**
Tel: +49-89-3 70 03 99-0
Fax: +49-89-3 70 03 99-99

**Moxa Asia-Pacific**
Tel: +886-2-8919-1230
Fax: +886-2-8919-1231

# Table of Contents


**1. Introduction ..... 1-1**
Overview ..... 1-2
Package Checklist ..... 1-2
Features ..... 1-2
Industrial Networking Capability ..... 1-2
Designed for Industrial Applications ..... 1-2
Useful Utility and Remote Configuration ..... 1-2

**2. Getting Started ..... 2-1**
RS-232 Console Configuration (115200, None, 8, 1, VT100) ..... 2-2
Using Telnet to Access the Industrial Secure Router's Console ..... 2-3
Using a Web Browser to Configure the Industrial Secure Router ..... 2-4

**3. Features and Functions ..... 3-1**
Overview ..... 3-2
Quick Setting Profile (EDR-810 series only) ..... 3-3
Configuring Basic Settings ..... 3-6
System Identification ..... 3-6
Accessible IP ..... 3-7
Password ..... 3-9
Time ..... 3-10
SettingCheck ..... 3-12
System File Update—by Remote TFTP ..... 3-13
System File Update—by Local Import/Export ..... 3-14
Restart ..... 3-15
Reset to Factory Default ..... 3-15
Configuring Ports (EDR-810 series only) ..... 3-15
Port Settings ..... 3-15
Using Port Trunk (EDR-810 series only) ..... 3-16
Port Trunk Settings ..... 3-17
Port Trunk Table ..... 3-17
Using Virtual LAN (EDR-810 series only) ..... 3-18
What is a VLAN? ..... 3-18
Benefits of VLANs ..... 3-18
Managing a VLAN ..... 3-19
Configuring Virtual LAN (EDR-810 Only) ..... 3-19
802.1Q VLAN Settings ..... 3-19
Quick Setting Panel ..... 3-20
VLAN Management ..... 3-20
Network Settings ..... 3-21
Mode Configuration (EDR-G902/G903 only) ..... 3-21
Network Mode ..... 3-21
Router Mode ..... 3-21
Bridge Mode ..... 3-21
WAN1 Configuration ..... 3-22
WAN2 Configuration (includes DMZ Enable, EDR-G903 only) ..... 3-24
Using DMZ Mode ..... 3-27
LAN Interface (EDR-G902/G903) ..... 3-28
LAN Configuration (EDR-810 series only) ..... 3-29
LAN Configuration ..... 3-29
DHCP Server ..... 3-29
Static DHCP List ..... 3-30
DHCP Leased List ..... 3-31
Dynamic DNS ..... 3-31
Network Redundancy ..... 3-32
WAN Backup (EDR-G903 only) ..... 3-32
How Dual WAN Backup Works ..... 3-32
WAN Backup Configuration ..... 3-33
Virtual Router Redundancy Protocol (VRRP) ..... 3-34
VRRP Settings ..... 3-34
Static Routing and Dynamic Routing ..... 3-35
Static Routing ..... 3-35
RIP (Routing Information Protocol) ..... 3-36
Routing Table ..... 3-37
Network Address Translation (NAT) ..... 3-37
NAT Concept ..... 3-37
N-to-1 NAT ..... 3-37
Port Forwarding (NAT Mode option) ..... 3-39
1-to-1 NAT ..... 3-40

Firewall Settings ..... 3-42
Firewall Policy Concept ..... 3-42
Firewall Policy Overview ..... 3-42
Firewall Policy Configuration ..... 3-43
Layer 2 Policy Setup (Only in Bridge Mode for EDR-G902/G903) ..... 3-44
Quick Automation Profile ..... 3-46
PolicyCheck ..... 3-48
Modbus TCP Policy Concept ..... 3-50
Modbus Policy Setup ..... 3-50
Denial of Service (DoS) function ..... 3-53
VPN (Virtual Private Network, EDR-G902/G903 and EDR-810-VPN only) ..... 3-54
Overview ..... 3-54
IPSec Configuration ..... 3-54
Global Configuration ..... 3-55
All IPSec Connection ..... 3-55
IPSec NAT-T ..... 3-55
IPSec Quick Setting ..... 3-55
IPSec Advanced Setting ..... 3-55
Tunnel Setting ..... 3-56
Key Exchange (IPSec phase I) ..... 3-57
Data Exchange (IPSec phase II) ..... 3-59
Dead Peer Detection ..... 3-59
IPSec Status ..... 3-60
X.509 Certification ..... 3-60
Certificate Generation ..... 3-61
Certificate Setting ..... 3-61
Local Certificate Upload ..... 3-62
Remote Certificate Upload ..... 3-62
L2TP (Layer 2 Tunnel Protocol) ..... 3-63
L2TP Configuration ..... 3-63
Examples for Typical VPN Applications ..... 3-64
Site to Site IPSec VPN tunnel with Pre-Shared Key ..... 3-64
VPN Plan ..... 3-64
L2TP for Remote User Maintenance ..... 3-65
VPN Plan ..... 3-65
Traffic Prioritization ..... 3-65
How Traffic Prioritization Works ..... 3-66
Traffic Prioritization Configuration (EDR-G902/G903 series) ..... 3-66
Configuring SNMP ..... 3-69
Using Auto Warning ..... 3-71
Configuring Email Warning ..... 3-72
Event Type ..... 3-72
E-mail Setup ..... 3-73
Configuring Relay Warning ..... 3-74
Using Diagnosis ..... 3-75
Using Monitor ..... 3-76
Monitor by System ..... 3-76
Monitor by Port ..... 3-76
Using System Log ..... 3-77
Using EventLog ..... 3-77
Using Syslog ..... 3-78
Using HTTPs/SSL ..... 3-79
**A. MIB Groups ..... A-1**

# 1

# Introduction

Welcome to the Moxa Industrial Secure Router series, the EDR-G902, EDR-G902, and EDR-810. The all-in-one Firewall/NAT/VPN secure routers are designed for connecting Ethernet-enabled devices with network IP security.

The following topics are covered in this chapter:

- **Overview**
- **Package Checklist**
- **Features**
  - Industrial Networking Capability
  - Designed for Industrial Applications
  - Useful Utility and Remote Configuration

# Overview

As the world's network and information technology becomes more mature, the trend is to use Ethernet as the major communications interface in many industrial communications and automation applications. In fact, a entirely new industry has sprung up to provide Ethernet products that comply with the requirements of demanding industrial applications.

Moxa's Industrial Secure Router series is a Gigabit speed, all-in-one Firewall/VPN/Router for Ethernet security applications in sensitive remote control and monitoring networks. The Industrial Secure Router supports one WAN, one LAN, and a user-configurable WAN/DMZ interface (EDR-G903) that provides high flexibility for different applications, such as WAN redundancy or Data/FTP server security protection.

The Quick Automation Profile function of the Industrial Secure Router's firewall supports most common Fieldbus protocols, including EtherCAT, EtherNet/IP, FOUNDATION Fieldbus, Modbus/TCP, and PROFINET. Users can easily create a secure Ethernet Fieldbus network from a user-friendly web UI with a single click. In addition, wide temperature models are available that operate reliably in hazardous, -40 to 75°C environments.

# Package Checklist

The Industrial Secure Routers are shipped with the following items. If any of these items are missing or damaged, please contact your customer service representative for assistance.

- 1 Moxa Industrial Secure Router
- RJ45 to DB9 console port cable
- Protective caps for unused ports
- DIN rail mounting kit (attached to the Industrial Secure Router's rear panel by default)
- Hardware installation guide (printed)
- CD-ROM with user's manual and Windows utility
- Warranty card

# Features

## Industrial Networking Capability

- Router/Firewall/VPN all in one
- 1 WAN, 1 LAN, and 1 user-configurable WAN or DMZ interface
- Network address translation (N-to-1, 1-to-1, and port forwarding)

## Designed for Industrial Applications

- Dual WAN redundancy function
- Firewall with Quick Automation Profile for Fieldbus protocols
- Intelligent PolicyCheck and SettingCheck tools
- -40 to 75°C operating temperature (T models)
- Long-haul transmission distance of 40 km or 80 km (with optional mini-GBIC)
- Redundant, dual 12 to 48 VDC power inputs
- IP30, rugged high-strength metal case
- DIN rail or panel mounting ability

## Useful Utility and Remote Configuration

- Configurable using a Web browser and Telnet/Serial console
- Send ping commands to identify network segment integrity

# 2

# Getting Started

This chapter explains how to access the Industrial Secure Router for the first time. There are three ways to access the router: (1) serial console, (2) Telnet console, and (3) web browser. The serial console connection method, which requires using a short serial cable to connect the Industrial Secure Router to a PC's COM port, can be used if you do not know the Industrial Secure Router's IP address. The Telnet console and web browser connection methods can be used to access the Industrial Secure Router over an Ethernet LAN, or over the Internet. A web browser can be used to perform all monitoring and administration functions, but the serial console and Telnet console only provide basic functions.

The following topics are covered in this chapter:

- **RS-232 Console Configuration (115200, None, 8, 1, VT100)**
- **Using Telnet to Access the Industrial Secure Router's Console**
- **Using a Web Browser to Configure the Industrial Secure Router**

# RS-232 Console Configuration (115200, None, 8, 1, VT100)

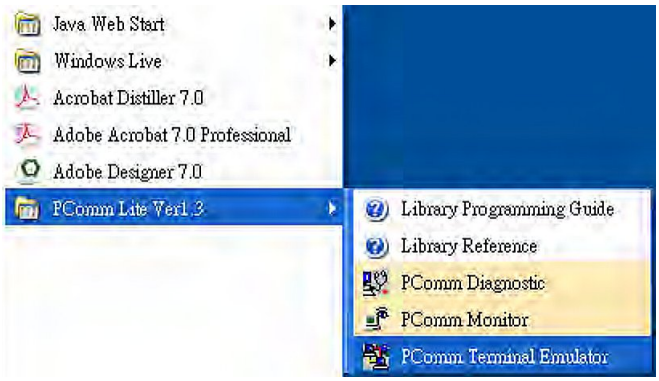
**NOTE** **Connection Caution!**
We strongly suggest that you do NOT use more than one connection method at the same time. Following this advice will allow you to maintain better control over the configuration of your Industrial Secure Router

**NOTE** We recommend using Moxa PComm Terminal Emulator, which can be downloaded free of charge from Moxa's website.

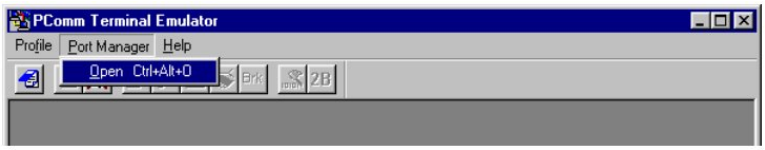
Before running PComm Terminal Emulator, use an RJ45 to DB9-F (or RJ45 to DB25-F) cable to connect the Industrial Secure Router's RS-232 console port to your PC's COM port (generally COM1 or COM2, depending on how your system is set up).

After installing PComm Terminal Emulator, perform the following steps to access the RS-232 console utility.

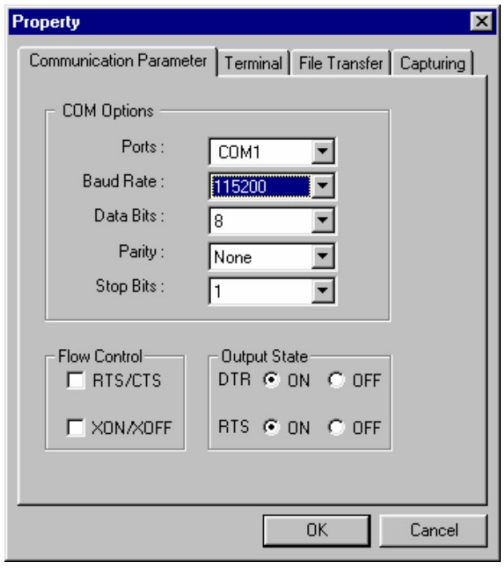
1. From the Windows desktop, click **Start** → **Programs** → **PCommLite1.3** → **Terminal Emulator**.



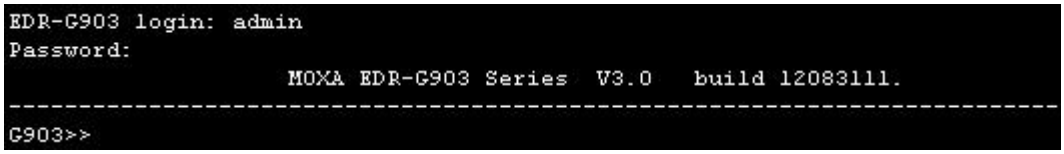

2. Select **Open** in the Port Manager menu to open a new connection.




3. The **Communication Parameter** page of the **Property** window will appear. Select the appropriate COM port from the **Ports** drop-down list, 115200 for Baud Rate, 8 for Data Bits, None for Parity, and 1 for Stop Bits.



4. Click the **Terminal** tab, select VT100 for Terminal Type, and then click **OK** to continue.
5. The **Console** login screen will appear. Use the keyboard to enter the login account (**admin** or **user**), and then press **Enter** to jump to the **Password** field. Enter the console Password (the same as the Web Browser password; leave the Password field blank if a console password has not been set), and then press **Enter**.




6. Enter a question mark (**?**) to display the command list in the console.

G903>>
quit - Exit Command Line Interface
exit - Exit Command Line Interface
reload - Halt and Perform a Cold Restart
terminal - Configure Terminal Page Length
copy - Import or Export File
save - Save Running Configuration to Flash
ping - Send Echo Messages
clear - Clear Information
show - Show System Information
configure - Enter Configuration Mode
G903>>

The following table lists commands that can be used when the Industrial Secure Router is in console (serial or Telnet) mode:

### Login by Admin Account

| Command | Description |
|---|---|
| quit | Exit Command Line Interface |
| exit | Exit Command Line Interface |
| reload | Halt and Perform a Cold Restart |
| terminal | Configure Terminal Page Length |
| copy | Import or Export File |
| save | Save Running Configuration to Flash |
| ping | Send Echo Messages |
| clear | Clear Information |
| show | Show System Information |
| configure | Enter Configuration Mode |

# Using Telnet to Access the Industrial Secure Router's Console

You may use Telnet to access the Industrial Secure Router's console utility over a network. To access the EDR's functions over the network (by either Telnet or a web browser) from a PC host that is connected to the same LAN as the Industrial Secure Router, you need to make sure that the PC host and the Industrial Secure Router are on the same logical subnet. To do this, check your PC host's IP address and subnet mask. By default, the LAN IP address is 192.168.127.254 and the Industrial subnet mask is 255.255.255.0 (for a Class C subnet). If you do not change these values, and your PC host's subnet mask is 255.255.0.0, then its IP address must have the form 192.168.xxx.xxx. On the other hand, if your PC host's subnet mask is 255.255.255.0, then its IP address must have the form, 192.168.127.xxx.

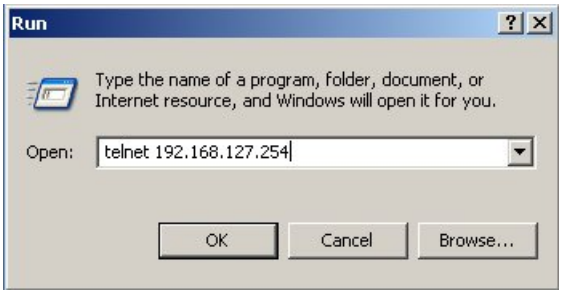
**NOTE** To use the Industrial Secure Router's management and monitoring functions from a PC host connected to the same LAN as the Industrial Secure Router, you must make sure that the PC host and the Industrial Secure Router are connected to the same logical subnet.

**NOTE** Before accessing the console utility via Telnet, first connect the Industrial Secure Router's RJ45 Ethernet LAN ports to your Ethernet LAN, or directly to your PC's Ethernet card (NIC). You can use either a straight-through or cross-over Ethernet cable.

**NOTE** The Industrial Secure Router's default LAN IP address is 192.168.127.254.

Perform the following steps to access the console utility via Telnet.

1. Click **Star**t → **Run**, and then telnet to the Industrial Secure Router's IP address from the Windows Run window. (You may also issue the Telnet command from the MS-DOS prompt.)




2. Refer to instructions 6 and 7 in the **RS-232 Console Configuration (115200, None, 8, 1, VT100)** section on page 2-2.

# Using a Web Browser to Configure the Industrial Secure Router

The Industrial Secure Router's web browser interface provides a convenient way to modify the router's configuration and access the built-in monitoring and network administration functions. The recommended web browser is Microsoft Internet Explorer 6.0 with JVM (Java Virtual Machine) installed.

**NOTE** To use the Industrial Secure Router's management and monitoring functions from a PC host connected to the same LAN as the Industrial Secure Router, you must make sure that the PC host and the Industrial Secure Router are connected to the same logical subnet.

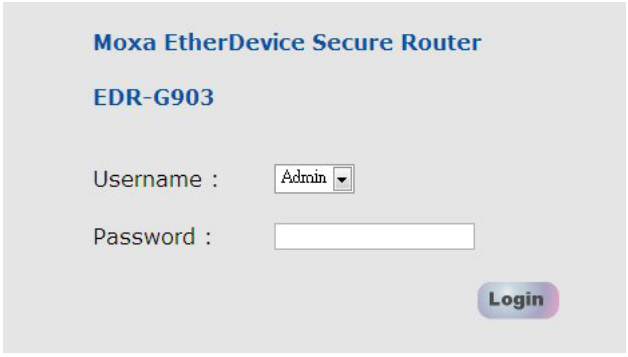
**NOTE** Before accessing the Industrial Secure Router's web browser, first connect the Industrial Secure Router's RJ45 Ethernet LAN ports to your Ethernet LAN, or directly to your PC's Ethernet card (NIC). You can use either a straight-through or cross-over Ethernet cable.

**NOTE** The Industrial Secure Router's default LAN IP address is 192.168.127.254.

Perform the following steps to access the Industrial Secure Router's web browser interface.

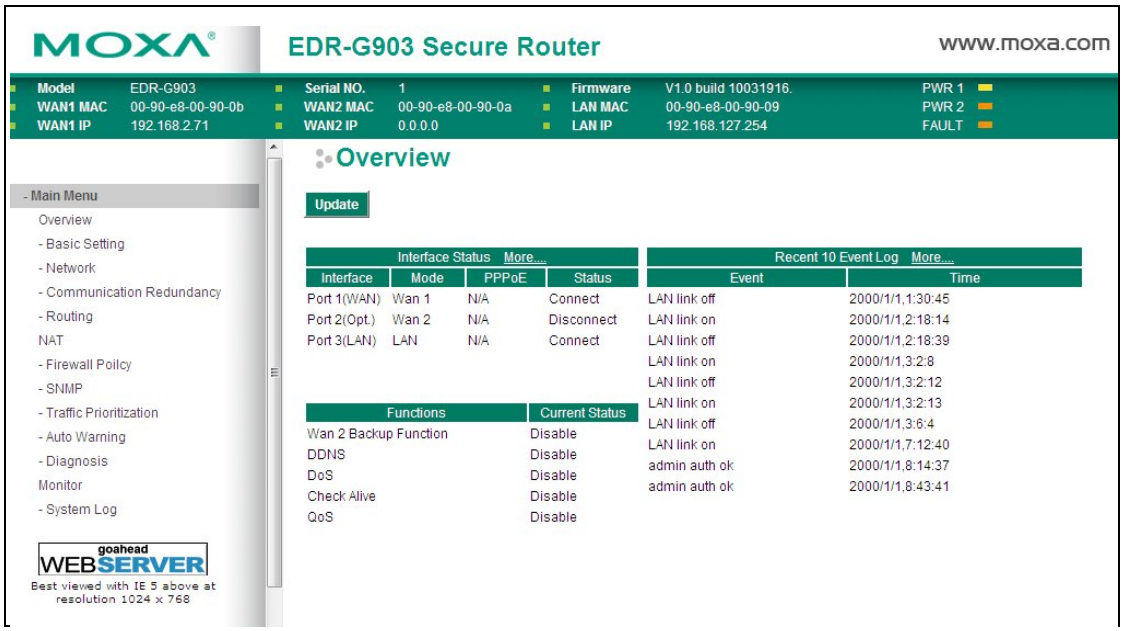
1. Start Internet Explorer and type the Industrial Secure Router's LAN IP address in the Address field. Press Enter to establish the connection.

2. The web login page will open. Select the login account (Admin or User) and enter the **Password** (the same as the Console password), and then click Login to continue. Leave the **Password** field blank if a password has not been set.




**NOTE** By default, the Industrial Secure Router's password is not set (i.e., is blank).

You may need to wait a few moments for the web page to be downloaded to your computer. Use the menu tree on the left side of the window to open the function pages to access each of the router's functions.



# 3

# Features and Functions

In this chapter, we explain how to access the Industrial Secure Router's configuration options, perform monitoring, and use administration functions. There are three ways to access these functions: (1) RS-232 console, (2) Telnet console, and (3) web browser.

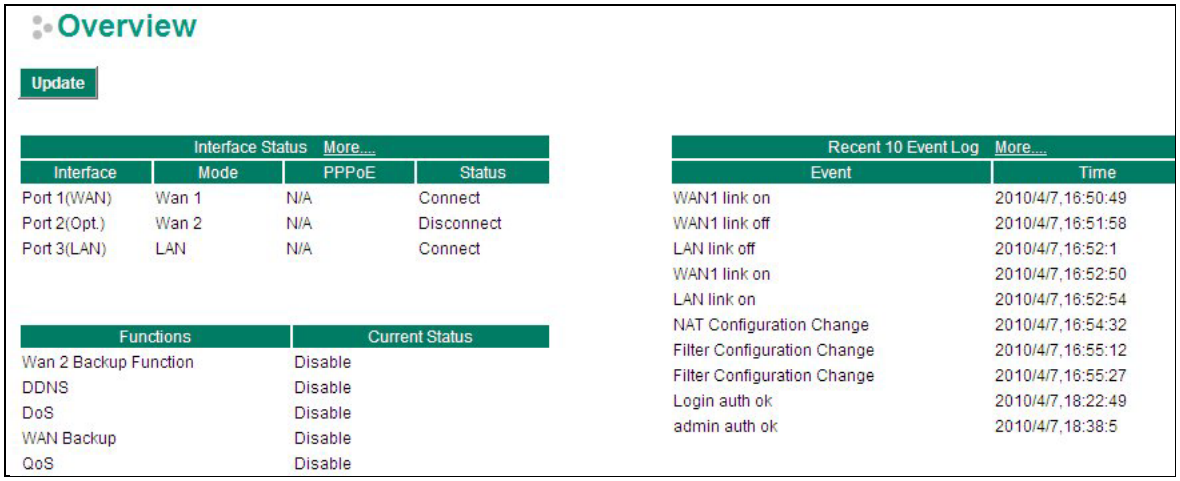
The web browser is the most user-friendly way to configure the Industrial Secure Router, since you can both monitor the Industrial Secure Router and use administration functions from the web browser. An RS-232 or Telnet console connection only provides basic functions. In this chapter, we use the web browser to introduce the Industrial Secure Router's configuration and monitoring functions.

The following topics are covered in this chapter:

- **Overview**
- **Quick Setting Profile (EDR-810 only)**
- **Configuring Basic Settings**
- **Configuring Ports (EDR-810 series only)**
- **Using Port Trunk (EDR-810 series only)**
- **Using Virtual LAN (EDR-810 series only)**
- **Configuring Virtual LAN (EDR-810 Only)**
- **Network Settings**
- **LAN Configuration (EDR-810 only)**
- **Network Redundancy**
- **Static Routing and Dynamic Routing**
- **Network Address Translation (NAT)**
- **Firewall Settings**
- **VPN (Virtual Private Network, EDR-G902/G903 and EDR-810-VPN only)**
- **Traffic Prioritization**
- **Configuring SNMP**
- **Using Auto Warning**
- **Using Diagnosis**
- **Using Monitor**
- **Using System Log**
- **Using HTTPs/SSL**

# Overview

The **Overview** page is divided into three major parts: **Interface Status**, **Basic function Status**, and **Recent 10 Event Log**, and gives users a quick overview of the Industrial Secure Router's current settings.



Overview

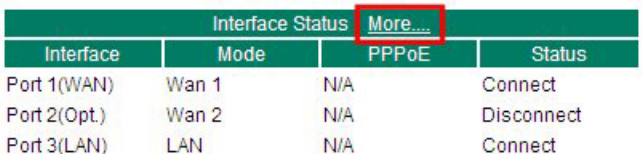
Update

| Interface Status More.... | | | |
|---|---|---|---|
| Interface | Mode | PPPoE | Status |
| Port 1(WAN) | Wan 1 | N/A | Connect |
| Port 2(Opt.) | Wan 2 | N/A | Disconnect |
| Port 3(LAN) | LAN | N/A | Connect |

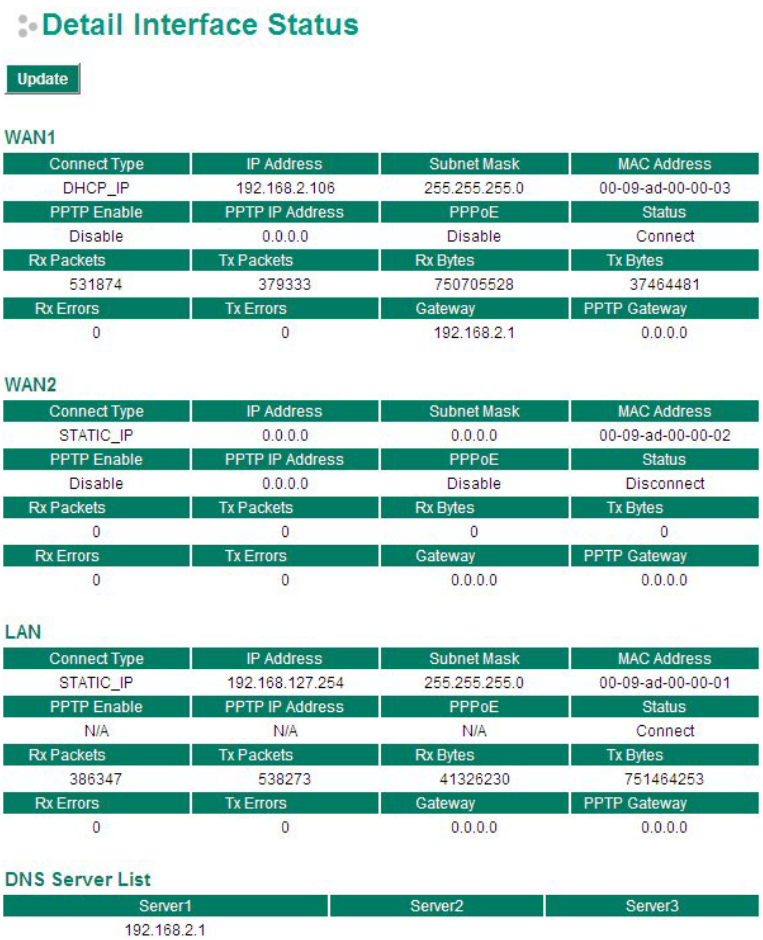
| Functions | Current Status |
|---|---|
| Wan 2 Backup Function | Disable |
| DDNS | Disable |
| DoS | Disable |
| WAN Backup | Disable |
| QoS | Disable |

| Recent 10 Event Log More.... | |
|---|---|
| Event | Time |
| WAN1 link on | 2010/4/7,16:50:49 |
| WAN1 link off | 2010/4/7,16:51:58 |
| LAN link off | 2010/4/7,16:52:1 |
| WAN1 link on | 2010/4/7,16:52:50 |
| LAN link on | 2010/4/7,16:52:54 |
| NAT Configuration Change | 2010/4/7,16:54:32 |
| Filter Configuration Change | 2010/4/7,16:55:12 |
| Filter Configuration Change | 2010/4/7,16:55:27 |
| Login auth ok | 2010/4/7,18:22:49 |
| admin auth ok | 2010/4/7,18:38:5 |

Click **More...** at the top of the Interface Status table to see detailed information about all interfaces.



| Interface Status More.... | | | |
|---|---|---|---|
| Interface | Mode | PPPoE | Status |
| Port 1(WAN) | Wan 1 | N/A | Connect |
| Port 2(Opt.) | Wan 2 | N/A | Disconnect |
| Port 3(LAN) | LAN | N/A | Connect |



Detail Interface Status

Update

WAN1

| Connect Type | IP Address | Subnet Mask | MAC Address |
|---|---|---|---|
| DHCP_IP | 192.168.2.106 | 255.255.255.0 | 00-09-ad-00-00-03 |
| PPTP Enable | PPTP IP Address | PPPoE | Status |
| Disable | 0.0.0.0 | Disable | Connect |
| Rx Packets | Tx Packets | Rx Bytes | Tx Bytes |
| 531874 | 379333 | 750705528 | 37464481 |
| Rx Errors | Tx Errors | Gateway | PPTP Gateway |
| 0 | 0 | 192.168.2.1 | 0.0.0.0 |

WAN2

| Connect Type | IP Address | Subnet Mask | MAC Address |
|---|---|---|---|
| STATIC_IP | 0.0.0.0 | 0.0.0.0 | 00-09-ad-00-00-02 |
| PPTP Enable | PPTP IP Address | PPPoE | Status |
| Disable | 0.0.0.0 | Disable | Disconnect |
| Rx Packets | Tx Packets | Rx Bytes | Tx Bytes |
| 0 | 0 | 0 | 0 |
| Rx Errors | Tx Errors | Gateway | PPTP Gateway |
| 0 | 0 | 0.0.0.0 | 0.0.0.0 |

LAN

| Connect Type | IP Address | Subnet Mask | MAC Address |
|---|---|---|---|
| STATIC_IP | 192.168.127.254 | 255.255.255.0 | 00-09-ad-00-00-01 |
| PPTP Enable | PPTP IP Address | PPPoE | Status |
| N/A | N/A | N/A | Connect |
| Rx Packets | Tx Packets | Rx Bytes | Tx Bytes |
| 386347 | 538273 | 41326230 | 751464253 |
| Rx Errors | Tx Errors | Gateway | PPTP Gateway |
| 0 | 0 | 0.0.0.0 | 0.0.0.0 |

DNS Server List

| Server1 | Server2 | Server3 |
|---|---|---|
| 192.168.2.1 | | |

Click **More...** at the top of the **Recent 10 Event Log"**table to open the **EventLogTable** page.

| Recent 10 Event Log | More.... |
|---|---|
| Event | Time |
| WAN1 link on | 2010/4/7,16:50:49 |
| WAN1 link off | 2010/4/7,16:51:58 |
| LAN link off | 2010/4/7,16:52:1 |

EventLogTable

Page 36/36

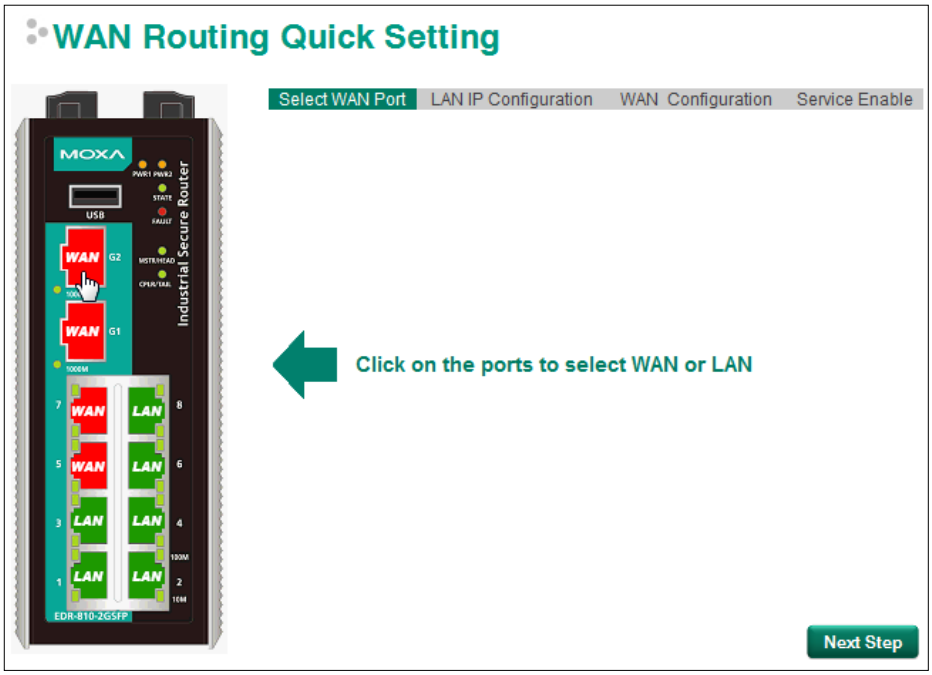
| Index | Bootup | Date | Time | System Startup Time | Event |
|---|---|---|---|---|---|
| 351 | 63 | 2010/4/7 | 16:52:1 | 0d0h13m7s | LAN link off |
| 352 | 63 | 2010/4/7 | 16:52:50 | 0d0h13m56s | WAN1 link on |
| 353 | 63 | 2010/4/7 | 16:52:54 | 0d0h14m0s | LAN link on |
| 354 | 63 | 2010/4/7 | 16:54:32 | 0d0h15m38s | NAT Configuration Change |
| 355 | 63 | 2010/4/7 | 16:55:12 | 0d0h16m18s | Filter Configuration Change |
| 356 | 63 | 2010/4/7 | 16:55:27 | 0d0h16m33s | Filter Configuration Change |
| 357 | 63 | 2010/4/7 | 18:22:49 | 0d1h43m55s | Login auth ok |
| 358 | 63 | 2010/4/7 | 18:38:5 | 0d1h59m11s | admin auth ok |

# Quick Setting Profile (EDR-810 series only)

The EDR-810 series supports WAN Routing Quick Setting, which creates a routing function between LAN ports and WAN ports defined by users. Follow the wizard's instructions to configuring the LAN and WAN ports.

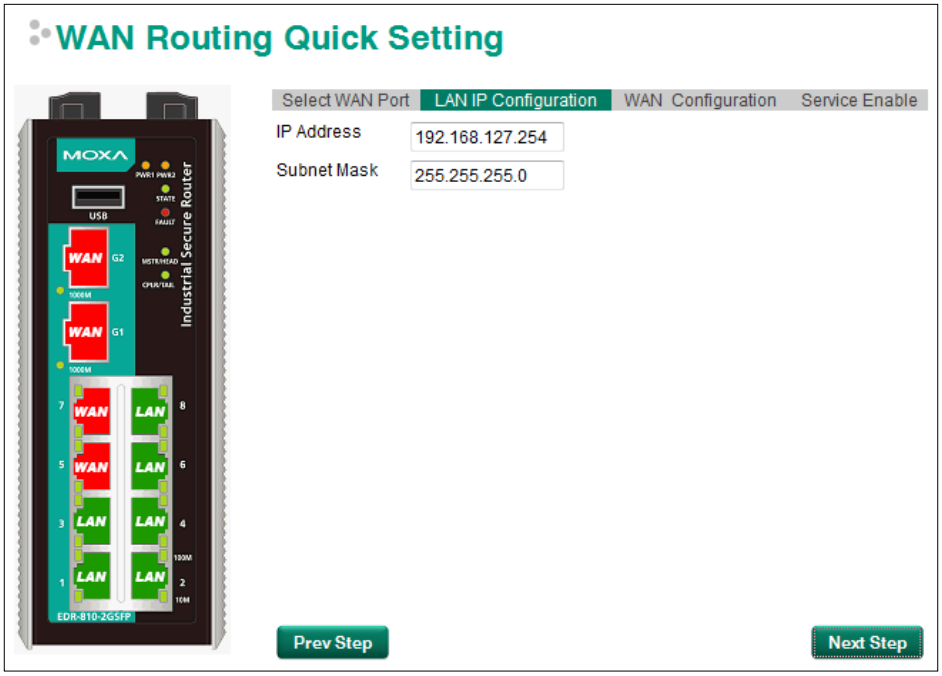
### Step 1: Define the WAN ports and LAN ports

Click on the ports in the figure to define the WAN ports and LAN ports.



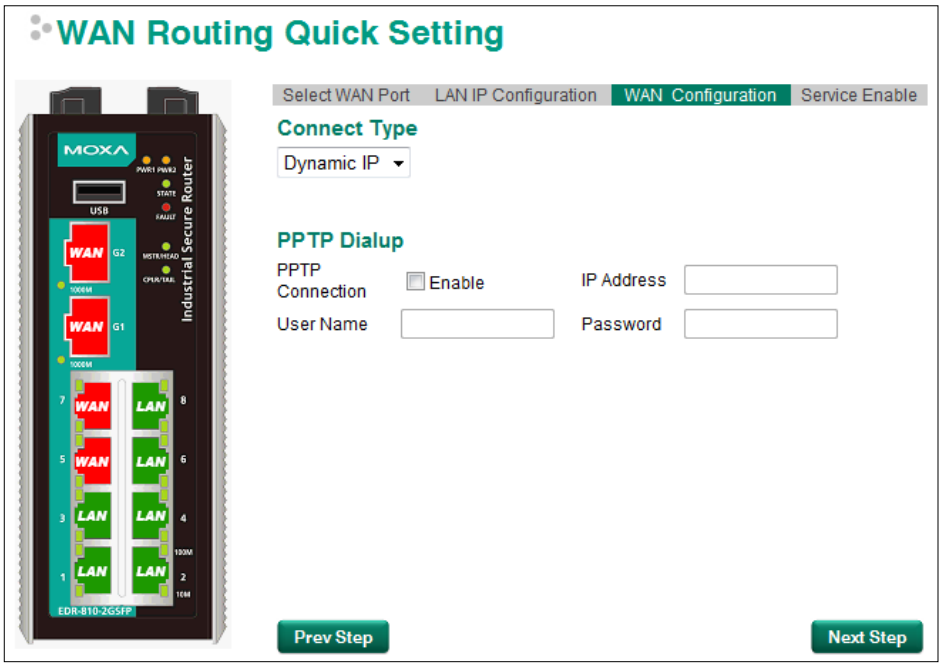
### Step 2: Configure the LAN IP address of the EDR-810 and the subnet address of the LAN ports

Configure the LAN IP address of the EDR-810 to define the subnet of the LAN ports on the secure router. The default IP address of the EDR-810 on the LAN side is 192.168.127.254, and the default subnet address is 192.168.127.0/24.




### Step 3: Configure the WAN port type

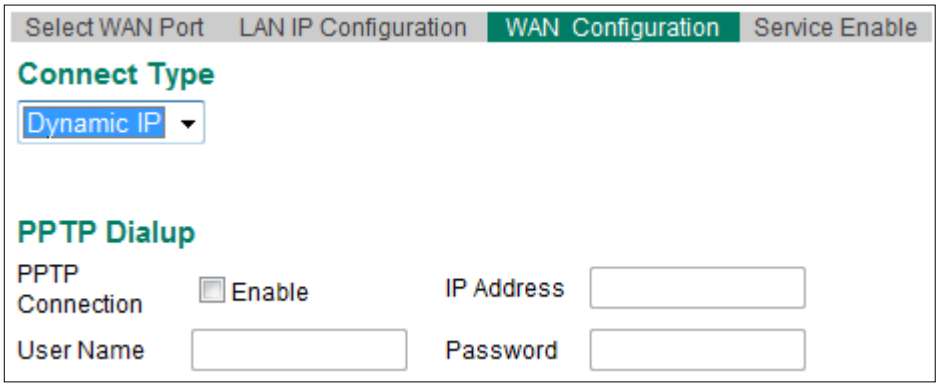
Configure the WAN port type to define how the secure router switch connects to the WAN.



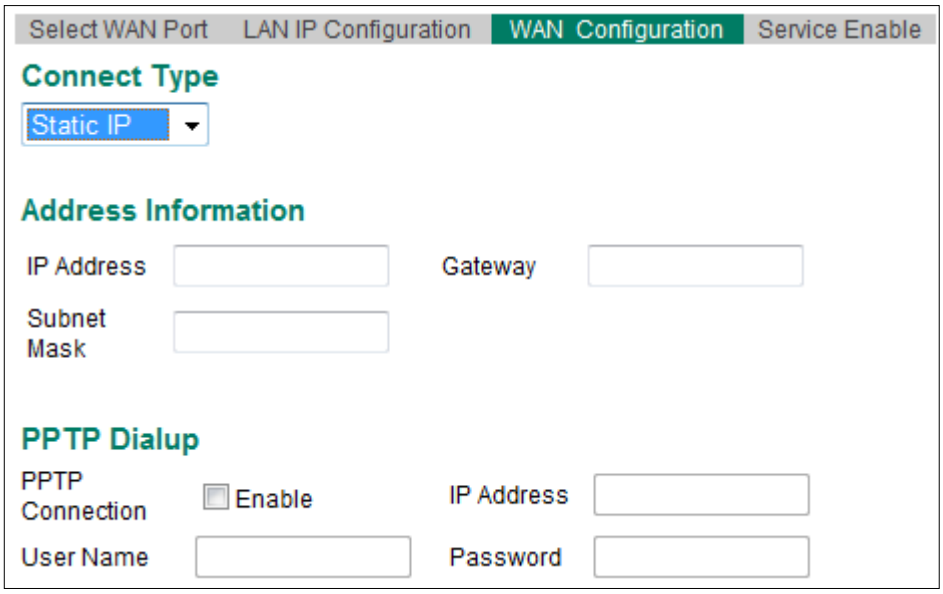

***Connect Type***

| Setting | Description | Factory Default |
|---|---|---|
| Dynamic IP | Get the WAN IP address from a DHCP server or via a PPTP connection. | Dynamic IP |
| Static IP | Set a specific static WAN IP address or create a connection to a PPTP server with a specific IP address. | |
| PPPoE | Get the WAN IP address through PPPoE Dialup. | |

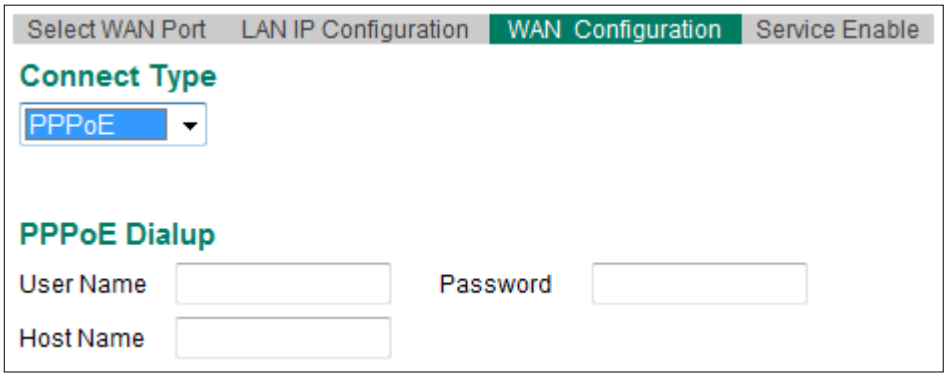
***Dynamic IP***




***Static IP***

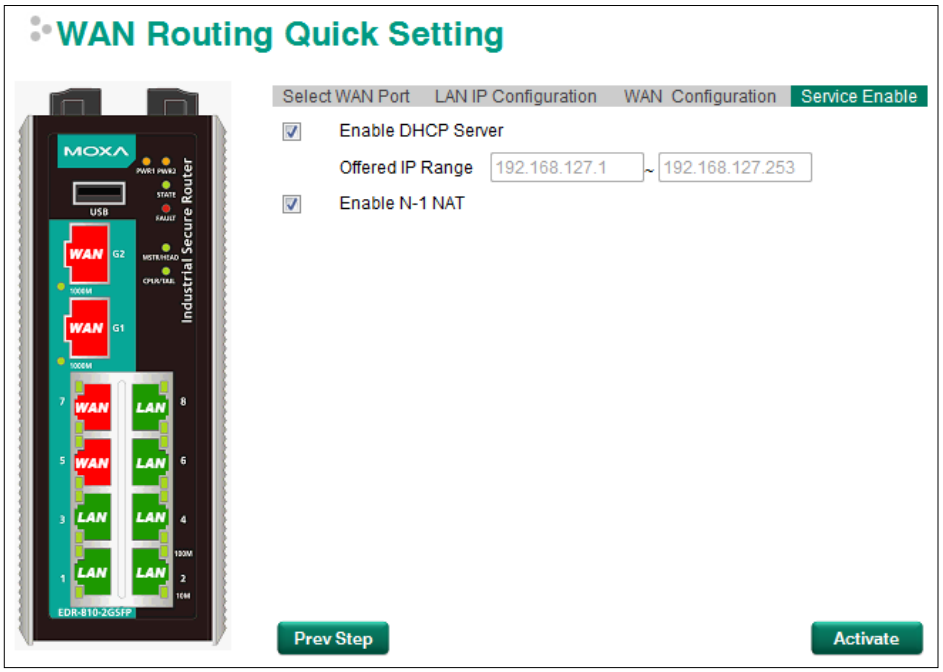



***PPPoE***



### Step 4: Enable services

Check **Enable DHCP Server** to enable the DHCP server for LAN devices. The default IP address range will be set automatically. To modify the IP range, go to the **DHCP Server** page. N-1 NAT will be also enabled by default.




### Step 5: Activate the settings

Click the **Activate** button.

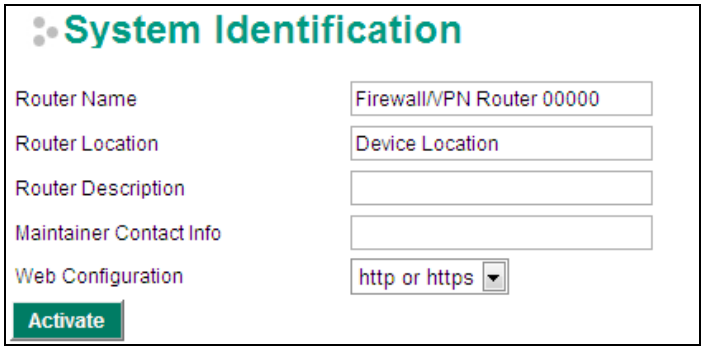
**NOTE** An existing configuration will be overwritten by new settings when processing **WAN Routing Quick Setting**.

# Configuring Basic Settings

The Basic Settings group includes the most commonly used settings required by administrators to maintain and control the Industrial Secure Router.

## System Identification

The system identification section gives you an easy way to identify the different switches connected to your network.



***Router name***

| Setting | Description | Factory Default |
|---|---|---|
| Max. 30 Characters | This option is useful for specifying the role or application of different Industrial Secure Router units.<br>E.g., Factory Router 1. | Firewall/VPN router [Serial No. of this switch] |

***Router Location***

| Setting | Description | Factory Default |
|---|---|---|
| Max. 80 Characters | To specify the location of different Industrial Secure Router units.<br>E.g., production line 1. | Device Location |

***Router Description***

| Setting | Description | Factory Default |
|---|---|---|
| Max. 30 Characters | Use this field to enter a more detailed description of the Industrial Secure Router unit. | None |

***Maintainer Contact Info***

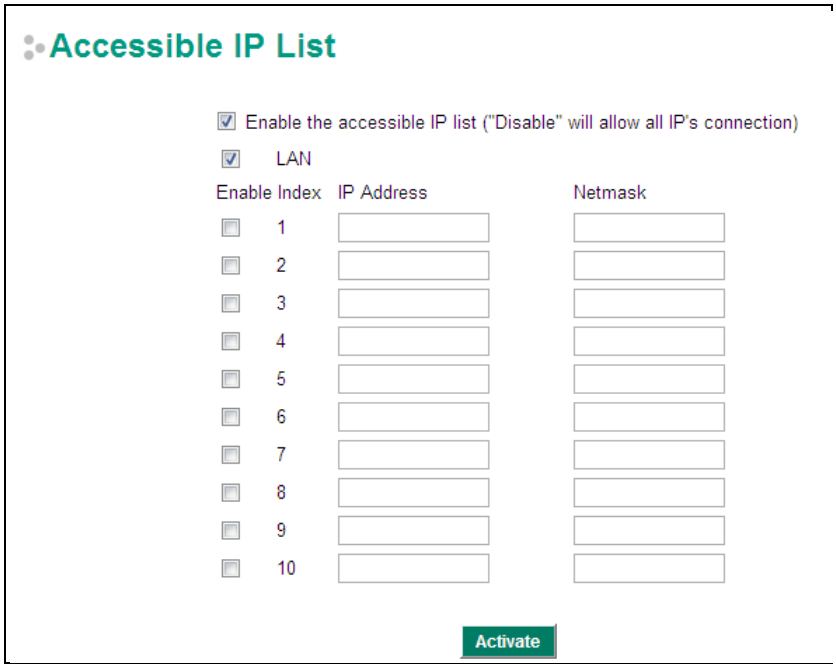
| Setting | Description | Factory Default |
|---|---|---|
| Max. 30 Characters | Enter the contact information of the person responsible for maintaining this Industrial Secure Router | None |

***Web Configuration***

| Setting | Description | Factory Default |
|---|---|---|
| http or https | Users can connect to the Industrial Secure Router router via http or https protocol. | http or https |
| https only | Users can connect to the Industrial Secure Router router via https protocol only. | |

# Accessible IP

The Industrial Secure Router uses an IP address-based filtering method to control access to Industrial Secure Router units.




Accessible IP Settings allows you to add or remove "Legal" remote host IP addresses to prevent unauthorized access. Access to the Industrial Secure Router is controlled by IP address. If a host's IP address is in the

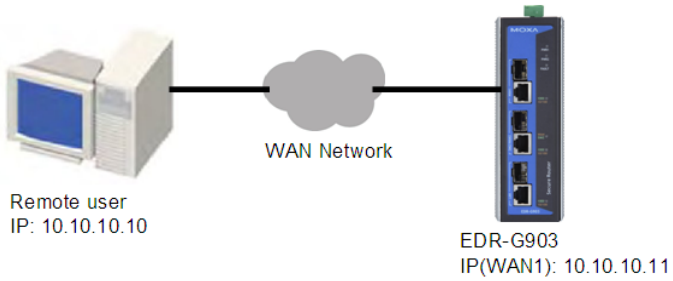
accessible IP table, then the host will have access to the Industrial Secure Router. You can allow one of the following cases by setting this parameter:

- Only one host with the specified IP address can access this device.
  E.g., enter "192.168.1.1/255.255.255.255" to allow access to just the IP address 192.168.1.1.
- Any host on a specific subnetwork can access this device.
  E.g., enter "192.168.1.0/255.255.255.0" to allow access to all IPs on the subnet defined by this IP address/subnet mask combination.
- Any host can access the Industrial Secure Router. (Disable this function by deselecting the Enable the accessible IP list option.)
- Any LAN can access the Industrial Secure Router. (Disable this function by deselecting the LAN option to not allow any IP at the LAN site to access this device.)
  E.g., If the LAN IP Address is set to 192.168.127.254/255.255.255.0, then IP addresses 192.168.127.1 /24 to 192.168.127.253/24 can access the Industrial Secure Router.

The following table shows additional configuration examples:

| **Allowable Hosts** | **Input Format** |
|---|---|
| Ay host | Disable |
| 192.168.1.120 | 192.168.1.120 / 255.255.255.255 |
| 192.168.1.1 to 192.168.1.254 | 192.168.1.0 / 255.255.255.0 |
| 192.168.0.1 to 192.168.255.254 | 192.168.0.0 / 255.255.0.0 |
| 192.168.1.1 to 192.168.1.126 | 192.168.1.0 / 255.255.255.128 |
| 192.168.1.129 to 192.168.1.254 | 192.168.1.128 / 255.255.255.128 |

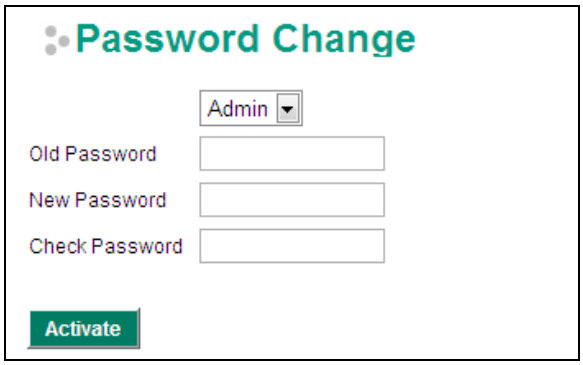
The Accessible IP list controls which devices can connect to the Industrial Secure Router to change the configuration of the device. In the example shown below, the Accessible IP list in the Industrial Secure Router contains 10.10.10.10, which is the IP address of the remote user's PC.




The remote user's IP address is shown below in the Industrial Secure Router's Accessible IP list.

# Password

The Industrial Secure Router provides two levels of access privilege: "admin privilege" gives read/write access to all Industrial Secure Router configuration parameters, and "user privilege" provides read access only. You will be able to view the configuration, but will not be able to make modifications.




**ATTENTION**

By default, the Password field is blank. If a Password is already set, then you will be required to type the Password when logging in to the RS-232 console, Telnet console, or web browser interface.

***Account***

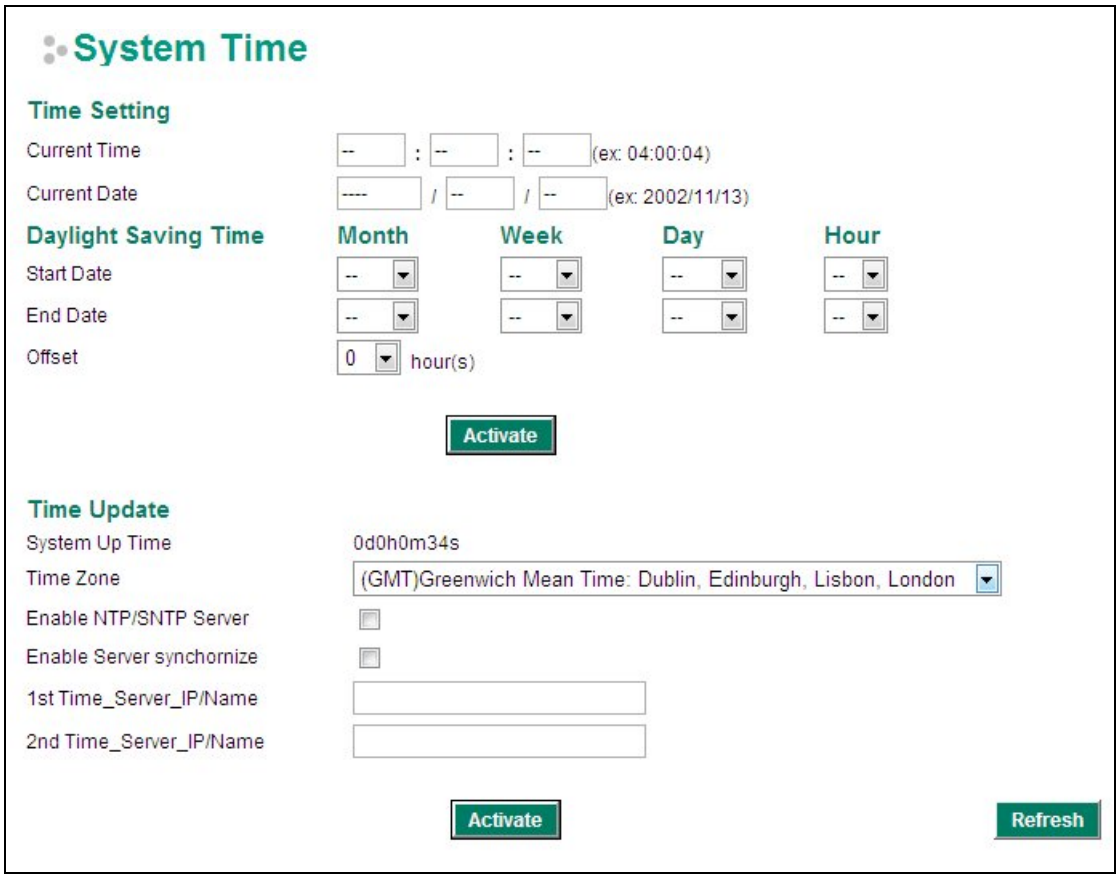
| Setting | Description | Factory Default |
|---|---|---|
| Admin | "admin" privilege allows the user to modify all configurations. | Admin |
| User | "user" privilege only allows viewing device configurations. | |

***Password***

| Setting | Description | Factory Default |
|---|---|---|
| Old password (max. 16 Characters) | Type current password when changing the password | None |
| New password (max. 16 Characters) | Type new password when changing the password | None |
| Retype password (max. 16 Characters) | If you type a new password in the Password field, you will be required to retype the password in the Retype new password field before updating the new password. | None |

# Time

The **Time** configuration page lets users set the time, date, and other settings. An explanation of each setting is given below.




The Industrial Secure Router has a time calibration function based on information from an NTP server or user specified Time and Date information. Functions such as Auto warning "Email" can add real-time information to the message.

**NOTE** The Industrial Secure Router has a real time clock so the user does not need to update the Current Time and Current Date to set the initial time for the Industrial Secure Router after each reboot. This is especially useful when the network does not have an Internet connection for an NTP server, or there is no NTP server on the network.

***Current Time***

| Setting | Description | Factory Default |
|---|---|---|
| User adjustable Time | The time parameter allows configuration of the local time in local 24-hour format. | None (hh:mm:ss) |

***Current Date***

| Setting | Description | Factory Default |
|---|---|---|
| User adjustable date. | The date parameter allows configuration of the local date in yyyy/mm/dd format | None (yyyy/mm/dd) |

***Daylight Savings Time***

Daylight Savings Time (also know as DST or summer time) involves advancing clocks 1 hour during the summer to provide an extra hour of daylight in the evening.

***Start Date***

| Setting | Description | Factory Default |
|---|---|---|
| User adjustable date. | The Start Date parameter allows users to enter the date that daylight saving time begins. | None |

***End Date***

| Setting | Description | Factory Default |
|---|---|---|
| User adjustable date. | The End Date parameter allows users to enter the date that daylight saving time begins. | None |

***Offset***

| Setting | Description | Factory Default |
|---|---|---|
| User adjustable date. | The offset parameter indicates how many hours forward the clock should be advanced. | None |

***System Up Time***

Indicates the ED-G903's up time from the last cold start. The unit is seconds.

***Time Zone***

| Setting | Description | Factory Default |
|---|---|---|
| User selectable time zone | The time zone setting allows conversion from GMT (Greenwich Mean Time) to local time. | GMT |

**NOTE** Changing the time zone will automatically correct the current time. You should **configure the time zone before setting the time**.

***Enable NTP/SNTP Server***

Enable this function to configure the Industrial Secure Router as an NTP/SNTP server on the network.

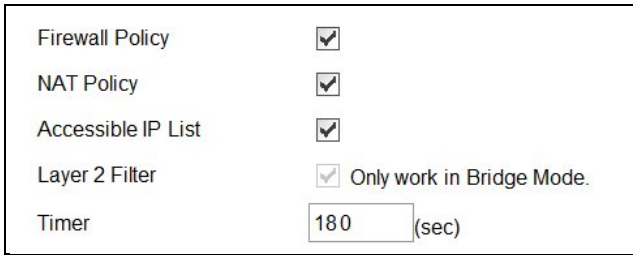
***Enable Server synchronize***

Enable this function to configure the Industrial Secure Router as an NTP/SNTP client, It will synchronize the time information with another NTP/SNTP server.

***Time Server IP/Name***

| Setting | Description | Factory Default |
|---|---|---|
| 1st Time Server IP/Name | IP or Domain address (e.g., 192.168.1.1, time.stdtime.gov.tw, or time.nist.gov). | None |
| 2nd Time Server IP/Name | The Industrial Secure Router will try to locate the 2nd NTP Server if the 1st NTP Server fails to connect. | |

# SettingCheck




**SettingCheck** is a safety function for industrial users using a secure router. It provides a double confirmation mechanism for when a remote user changes the security policies, such as **Firewall filter**, **NAT**, and **Accessible IP list**. When a remote user changes these security polices, SettingCheck provides a means of blocking the connection from the remote user to the Firewall/VPN device. The only way to correct a wrong setting is to get help from the local operator, or go to the local site and connect to the device through the console port, which could take quite a bit of time and money. Enabling the SettingCheck function will execute these new policy changes temporarily until doubly confirmed by the user. If the user does not click the confirm button, the Industrial Secure Router will revert to the previous setting.

***Firewall Policy***

Enables or Disables the SettingCheck function when the Firewall policies change.

***NAT Policy***

Enables or Disables the SettingCheck function when the NAT policies change.

***Accessible IP List***

Enables or Disables the SettingCheck function when the Accessible IP List changes.

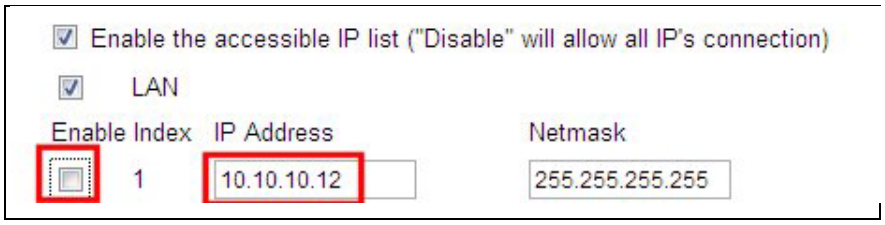
***Layer 2 Filter***

Enable or disable the SettingCheck function when the Layer 2 filter changes.

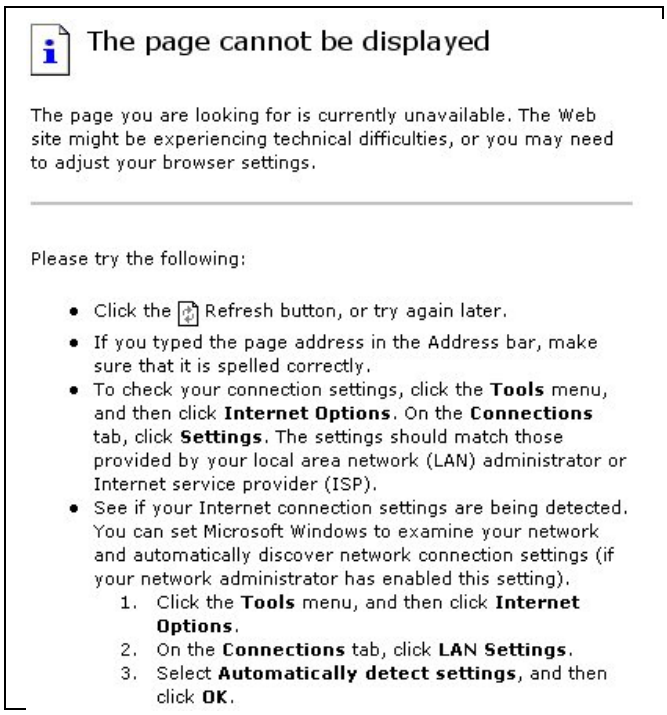
***Timer***

| Setting | Description | Factory Default |
|---|---|---|
| 10 to 3600 sec. | The timer waits this amount of time to double confirm when the user changes the policies | 180 (sec.) |

For example, if the remote user (IP: 10.10.10.10) connects to the Industrial Secure Router and changes the accessible IP address to 10.10.10.12, or deselects the Enable checkbox accidently after the remote user clicks the Activate button, connection to the Industrial Secure Router will be lost because the IP address is not in the Industrial Secure Router's Accessible IP list.



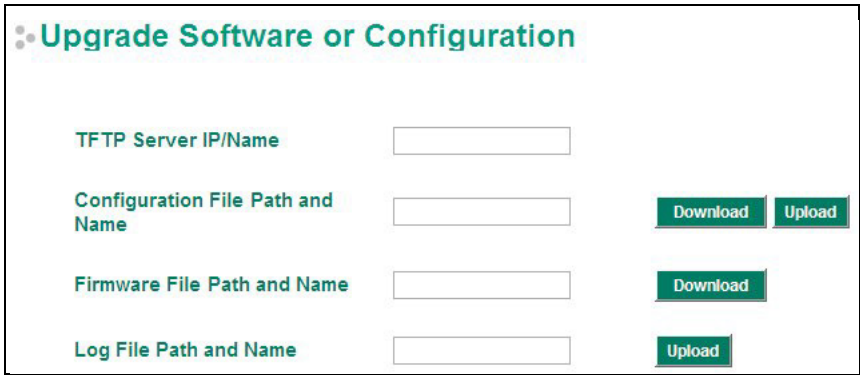

If the user enables the SettingCheck function with the Accessible IP list and the confirmer Timer is set to 15 seconds, then when the user clicks the Activate button on the accessible IP list page, the Industrial Secure Router will execute the configuration change and the web browser will try to jump to the SettingCheck Confirmed page automatically. Because the new IP list does not include the Remote user's IP address, the remote user cannot connect to the SettingCheck Confirmed page. After 15 seconds, the Industrial Secure Router will roll back to the original Accessible IP List setting, allowing the remote user to reconnect to the Industrial Secure Router and check what's wrong with the previous setting.


The page cannot be displayed
The page you are looking for is currently unavailable. The Web site might be experiencing technical difficulties, or you may need to adjust your browser settings.
Please try the following:
Click the Refresh button, or try again later.
If you typed the page address in the Address bar, make sure that it is spelled correctly.
To check your connection settings, click the Tools menu, and then click Internet Options. On the Connections tab, click Settings. The settings should match those provided by your local area network (LAN) administrator or Internet service provider (ISP).
See if your Internet connection settings are being detected. You can set Microsoft Windows to examine your network and automatically discover network connection settings (if your network administrator has enabled this setting).
1. Click the Tools menu, and then click Internet Options.
2. On the Connections tab, click LAN Settings.
3. Select Automatically detect settings, and then click OK.

If the new configuration does not block the connection from the remote user to the Industrial Secure Router, the user will see the SettingCheck Confirmed page, shown in the following figure. Click **Confirm** to save the configuration updates.

# System File Update—by Remote TFTP

The Industrial Secure Router supports saving your configuration file to a remote TFTP server or local host to allow other Industrial Secure Routers to use the same configuration at a later time, or saving the Log file for future reference. Loading pre-saved firmware or a configuration file from the TFTP server or local host is also supported to make it easier to upgrade or configure the Industrial Secure Router.




***TFTP Server IP/Name***

| Setting | Description | Factory Default |
|---|---|---|
| IP Address of TFTP Server | The IP or name of the remote TFTP server. Must be configured before downloading or uploading files. | None |

***Configuration File Path and Name***

| Setting | Description | Factory Default |
|---|---|---|
| Max. 40 Characters | The path and filename of the Industrial Secure Router's configuration file in the TFTP server. | None |

***Firmware File Path and Name***

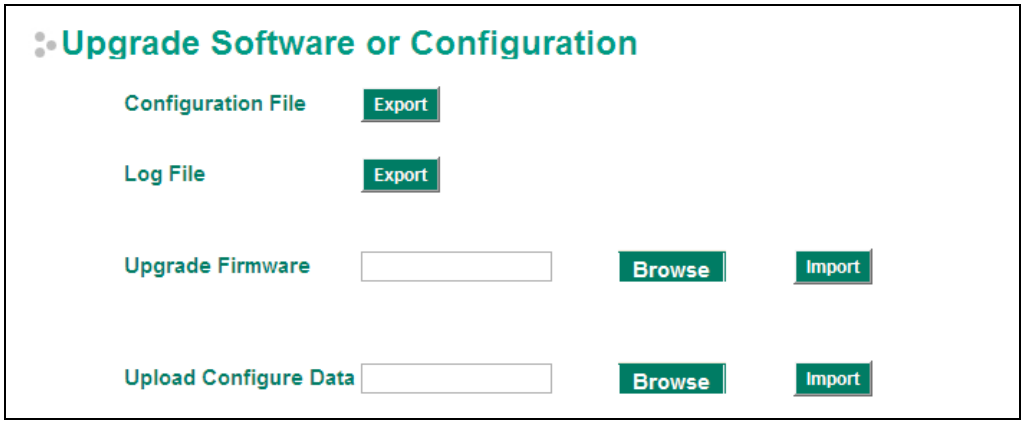
| Setting | Description | Factory Default |
|---|---|---|
| Max. 40 Characters | The path and filename of the Industrial Secure Router's firmware file | None |

***Log File Path and Name***

| Setting | Description | Factory Default |
|---|---|---|
| Max. 40 Characters | The path and filename of the Industrial Secure Router's log file | None |

After setting up the desired path and filename, click **Activate** to save the setting. Next, click **Download** to download the file from the remote TFTP server, or click **Upload** to upload a file to the remote TFTP server.

# System File Update—by Local Import/Export




***Configuration File***

Click **Export** to export the configuration file of the Industrial Secure Router to the local host.

***Log File***

Click **Export** to export the Log file of the Industrial Secure Router to the local host.

**NOTE** Some operating systems will open the configuration file and log file directly in the web page. In such cases, right click the **Export** button and then save as a file.

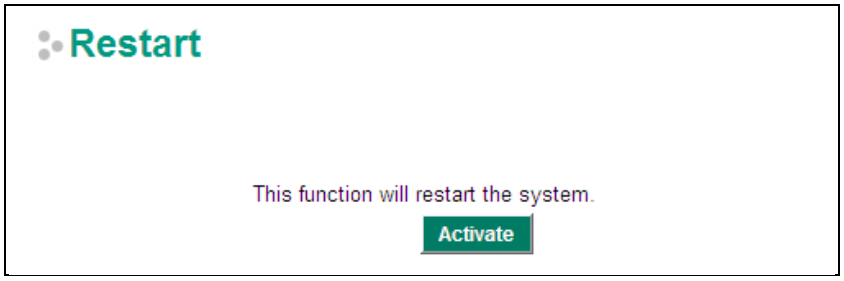
***Upgrade Firmware***

To import a firmware file into the Industrial Secure Router, click **Browse** to select a firmware file already saved on your computer. The upgrade procedure will proceed automatically after clicking Import. This upgrade procedure will take a couple of minutes to complete, including the boot-up time.

***Upload Configuration Data***

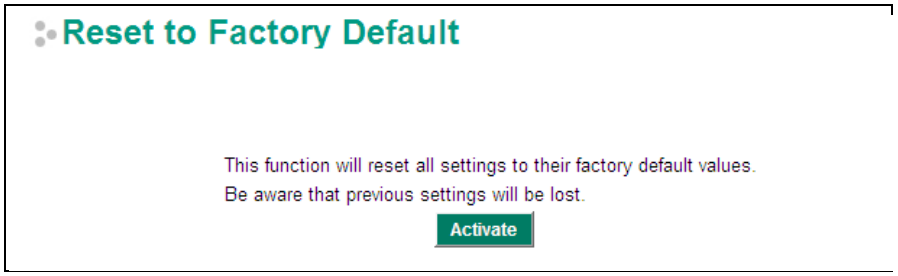
To import a configuration file to the Industrial Secure Router, click **Browse** to select a configuration file already saved on your computer. The upgrade procedure will proceed automatically after clicking Import.

## Restart




This function is used to restart the Industrial Secure Router.

## Reset to Factory Default


Reset to Factory Default
This function will reset all settings to their factory default values.
Be aware that previous settings will be lost.
Activate

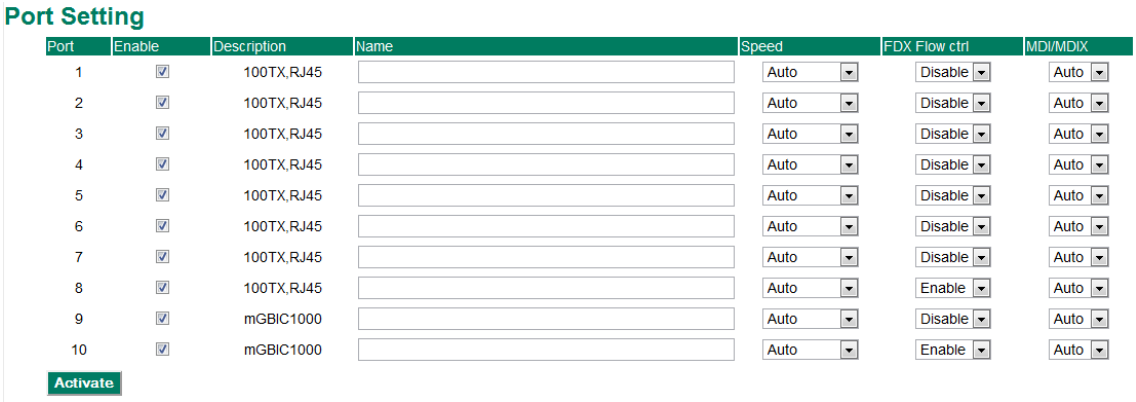
The **Reset to Factory Default** option gives users a quick way of restoring the Industrial Secure Router's configuration settings to the factory default values. This function is available in the console utility (serial or Telnet), and web browser interface.

**NOTE** After activating the Factory Default function, you will need to use the default network settings to re-establish a web-browser or Telnet connection with your Industrial Secure Router.

# Configuring Ports (EDR-810 series only)

## Port Settings

Port settings are included to give the user control over port access, port transmission speed, flow control, and port type (MDI or MDIX).


Port Setting
Port Enable Description Name Speed FDX Flow ctrl MDI/MDIX
1 100TX,RJ45 Auto Disable Auto
2 100TX,RJ45 Auto Disable Auto
3 100TX,RJ45 Auto Disable Auto
4 100TX,RJ45 Auto Disable Auto
5 100TX,RJ45 Auto Disable Auto
6 100TX,RJ45 Auto Disable Auto
7 100TX,RJ45 Auto Disable Auto
8 100TX,RJ45 Auto Enable Auto
9 mGBIC1000 Auto Disable Auto
10 mGBIC1000 Auto Enable Auto
Activate

***Enable***

| Setting | Description | Factory Default |
|---|---|---|
| Checked | Allows data transmission through the port. | Enabled |
| Unchecked | Immediately shuts off port access. | |

***Description***

| Setting | Description | Factory Default |
|---|---|---|
| Media Type | Displays the media type for each module's port | N/A |

***Name***

| Setting | Description | Factory Default |
|---|---|---|
| Max. 63 characters | Specifies an alias for the port to help administrators differentiate between different ports. Example: PLC 1 | None |

***Speed***

| Setting | Description | Factory Default |
|---|---|---|
| Auto | Allows the port to use the IEEE 802.3u protocol to negotiate with connected devices. The port and connected devices will determine the best speed for that connection. | Auto |
| 1G-Full | Choose one of these fixed speed options if the connected Ethernet device has trouble auto-negotiating for line speed. | |
| 100M-Full | | |
| 100M-Half | | |
| 10M-Full | | |
| 10M-Half | | |

***FDX Flow Ctrl***

This setting enables or disables flow control for the port when the port's Speed is set to Auto. The final result will be determined by the Auto process between the Moxa switch and connected devices.

| Setting | Description | Factory Default |
|---|---|---|
| Enable | Enables flow control for this port when the port's Speed is set to Auto. | Auto |
| Disable | Disables flow control for this port when the port's Speed is set to Auto. | |

***MDI/MDIX***

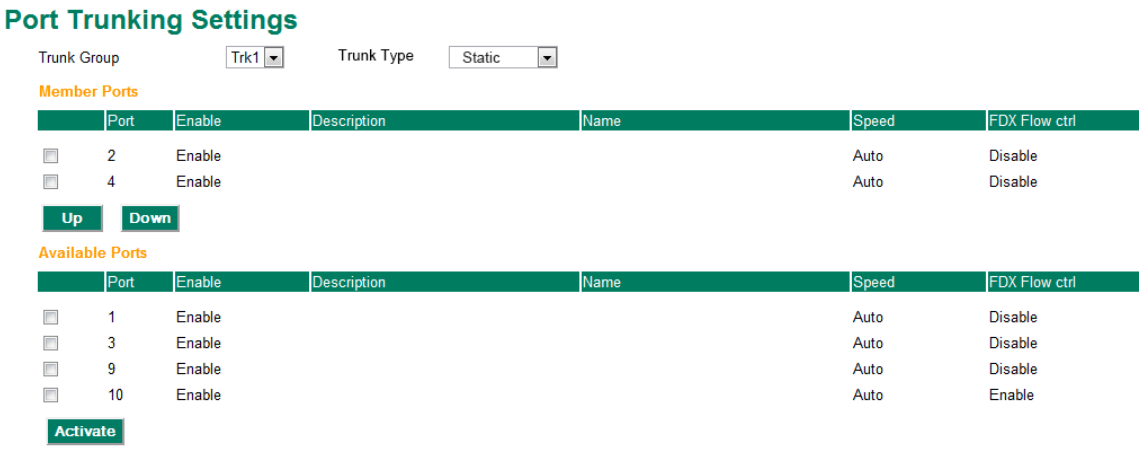
| Setting | Description | Factory Default |
|---|---|---|
| Auto | Allows the port to auto-detect the port type of the connected Ethernet device and change the port type accordingly. | Auto |
| MDI | Choose MDI or MDIX if the connected Ethernet device has trouble auto-negotiating for port type. | |
| MDIX | | |

# Using Port Trunk (EDR-810 series only)

Link aggregation involves grouping links into a link aggregation group. A MAC client can treat link aggregation groups as if they were a single link. The port trunking feature allows devices to communicate by aggregating up to 4 trunk groups, with a maximum of 8 ports for each group. If one of the 8 ports fails, the other seven ports will automatically provide backup and share the traffic. Port trunking can be used to combine up to 8 ports between two Moxa switches. If all ports on both switches are configured as 100BaseTX and they are operating in full duplex, the potential bandwidth of the connection will be 1600 Mbps.

# Port Trunk Settings

The **Port Trunking Settings** page is where ports are assigned to a trunk group.




**Step 1:** Select the desired **Trunk Group**.

**Step 2:** Select the **Trunk Type** (Static or LACP). **Note: LACP will be ready by Q4, 2013.**

**Step 3:** Select the desired ports under **Available Ports** and click **Up** to add to the Trunk Group.

**Step 4:** Select the desired ports under **Member Ports** and click **Down** to remove from the group.

**Step 5:** Click **Activate** to finish the settings.

***Trunk Group (maximum of four trunk groups)***

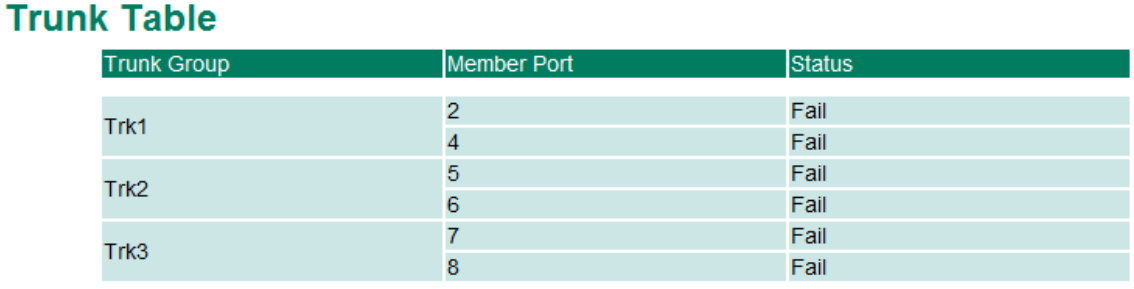
| Setting | Description | Factory Default |
|---|---|---|
| Trk1, Trk2, Trk3, Trk4 | Specifies the current trunk group. | Trk1 |

***Available Ports/Member Ports***

| Setting | Description | Factory Default |
|---|---|---|
| Member/Available Ports | List the ports in the current trunk group and the ports that are available to be added. | |
| Checkbox | Select the port to be added or removed from the group. | Unchecked |
| Port | How each port is identified. | |
| Port description | Displays the media type for each port. | |
| Name | Displays the specified name for each port. | |
| Speed | Indicates the transmission speed for each port. | |
| FDX flow control | Indicates if the FDX flow control of this port is enabled or disabled. | |
| Up | Add selected ports into the trunk group from available ports. | |
| Down | Remove selected ports from the trunk group. | |

# Port Trunk Table

The **Port Trunk Table** shows the current trunk status of configured trunk groups.



***Trunk Table***

| Setting | Description |
|---|---|
| Trunk group | Displays the trunk type and trunk group. |
| Member port | Displays the member ports that belong to the trunk group. |
| Status | • Success means port trunking is working properly.<br>• Fail means port trunking is not working properly.<br>• Standby means port trunking is working as a standby port. When there are more than eight ports trunked as a trunking group, the 9th port will be the standby port. |

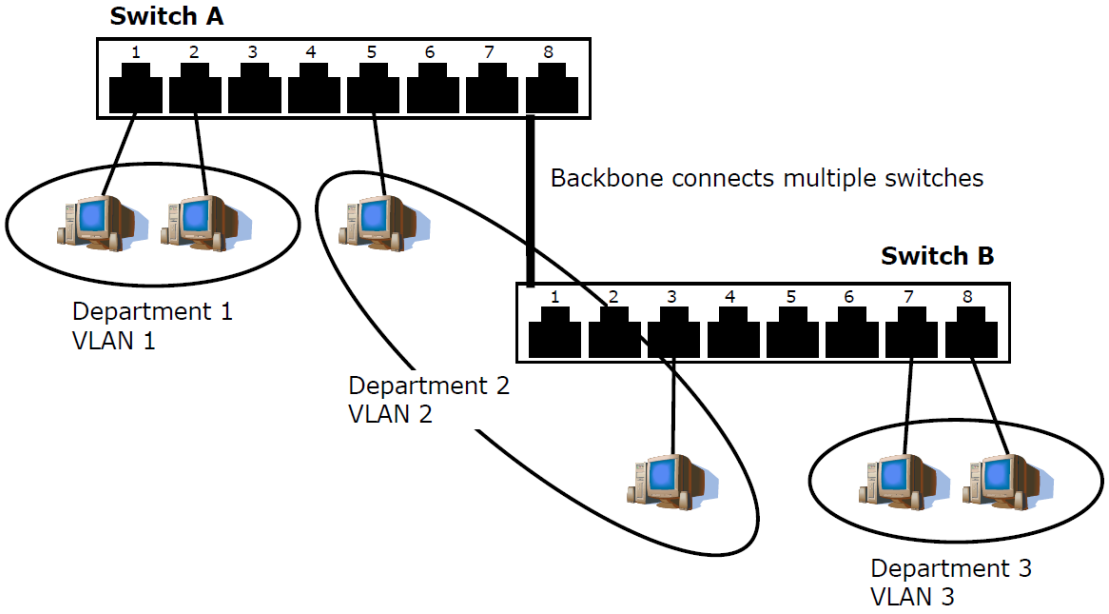
# Using Virtual LAN (EDR-810 series only)

Setting up Virtual LANs (VLANs) on your Moxa switch increases the efficiency of your network by dividing the LAN into logical segments, as opposed to physical segments. In general, VLANs are easier to manage.

## What is a VLAN?

A VLAN is a group of devices that can be located anywhere on a network, but which communicate as if they are on the same physical segment. With VLANs, you can segment your network without being restricted by physical connections—a limitation of traditional network design. With VLANs you can segment your network into:

- **Departmental groups**—you could have one VLAN for the marketing department, another for the finance department, and another for the product development department.
- **Hierarchical groups**—you could have one VLAN for directors, another for managers, and another for general staff.
- **Usage groups**—you could have one VLAN for email users and another for multimedia users.




## Benefits of VLANs

The main benefit of VLANs is that they provide a network segmentation system that is far more flexible than traditional networks. Using VLANs also provides you with three other benefits:

- **VLANs ease the relocation of devices on networks:** With traditional networks, network administrators spend much of their time dealing with moves and changes. If users move to a different sub-network, the addresses of each host must be updated manually. With a VLAN setup, if a host originally on VLAN

Marketing, for example, is moved to a port on another part of the network, and retains its original subnet membership, you only need to specify that the new port is on VLAN Marketing. You do not need to do any re-cabling.

- **VLANs provide extra security:** Devices within each VLAN can only communicate with other devices on the same VLAN. If a device on VLAN Marketing needs to communicate with devices on VLAN Finance, the traffic must pass through a routing device or Layer 3 switch.
- **VLANs help control traffic:** With traditional networks, congestion can be caused by broadcast traffic that is directed to all network devices, regardless of whether or not they need it. VLANs increase the efficiency of your network because each VLAN can be set up to contain only those devices that need to communicate with each other.

## Managing a VLAN

A new or initialized Moxa switch contains a single VLAN—the Default VLAN. This VLAN has the following definition:

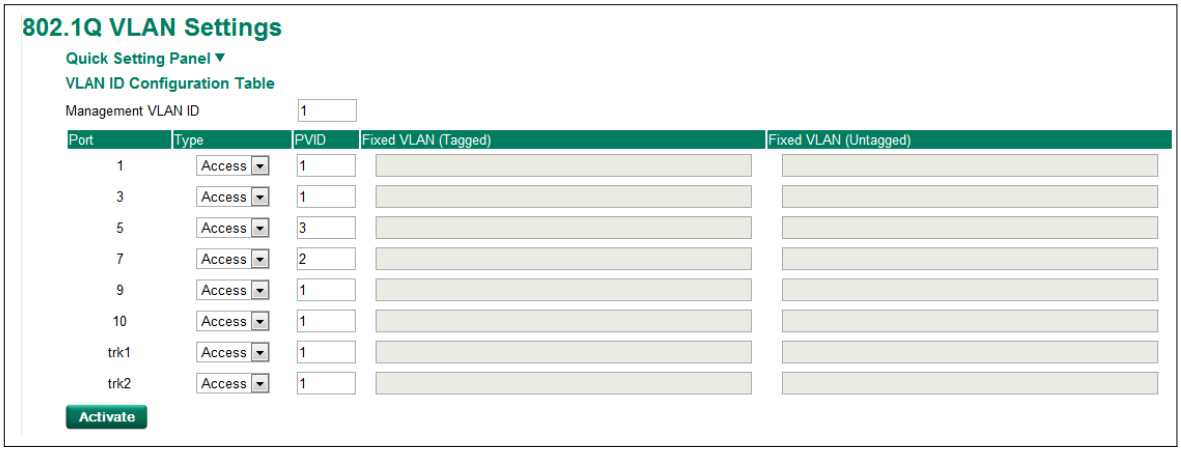
- **VLAN Name**—Management VLAN
- **802.1Q VLAN ID**—1 (if tagging is required)

All of the ports are initially placed on this VLAN, and it is the only VLAN that allows you to access the management software of the Moxa switch over the network.

# Configuring Virtual LAN (EDR-810 Only)

To configure **802.1Q VLAN** on the Moxa switch, use the **802.1Q VLAN Settings** page to configure the ports.

## 802.1Q VLAN Settings




***Management VLAN ID***

| Setting | Description | Factory Default |
|---|---|---|
| VLAN ID from 1-4094 | Assigns the VLAN ID of this Moxa switch. | 1 |

***Port Type***

| Setting | Description | Factory Default |
|---|---|---|
| Access | Port type is used to connect single devices without tags. | Access |
| Trunk | Select Trunk port type to connect another 802.1Q VLAN aware switch. | |
| Hybrid | Select Hybrid port to connect another Access 802.1Q VLAN aware switch or another LAN that combines tagged and/or untagged devices and/or other switches/hubs. | |

***PVID***

| Setting | Description | Factory Default |
|---|---|---|
| VLAN ID from 1-4094 | Sets the default VLAN ID for untagged devices that connect to the port. | 1 |

***Fixed VLAN (Tagged)***

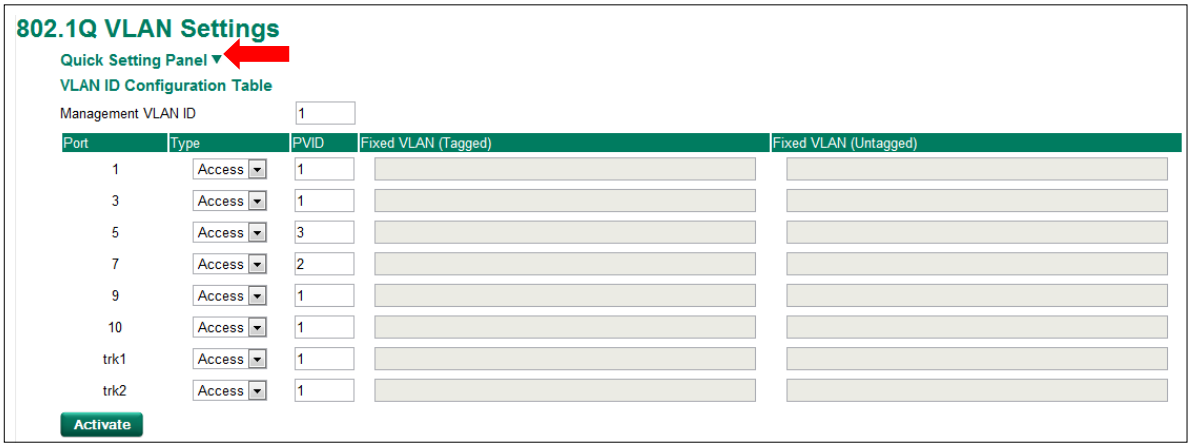
| Setting | Description | Factory Default |
|---|---|---|
| VLAN ID from 1-4094 | This field will be active only when selecting the Trunk or Hybrid port type. Set the other VLAN ID for tagged devices that connect to the port. Use commas to separate different VIDs. | None |

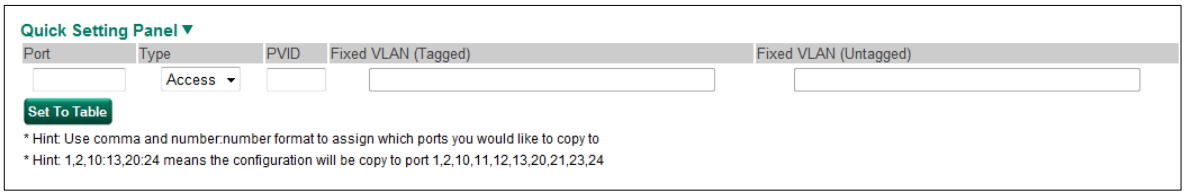
***Fixed VLAN (Untagged)***

| Setting | Description | Factory Default |
|---|---|---|
| VLAN ID from 1-4094 | This field will be active only when selecting the Trunk or Hybrid port type. Set the other VLAN ID for tagged devices that connect to the port and tags that need to be removed in egress packets. Use commas to separate different VIDs. | None |

# Quick Setting Panel

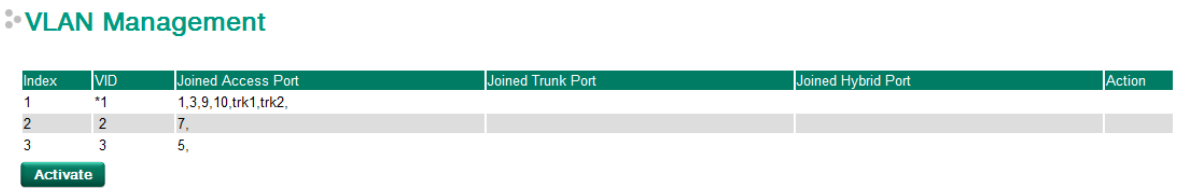
Click the triangle to open the **Quick Setting Panel**. Use this panel for quick and easy configuration of VLAN settings.





Quick Setting Panel
Port
Type
PVID
Fixed VLAN (Tagged)
Fixed VLAN (Untagged)
Access
Set To Table
* Hint: Use comma and number:number format to assign which ports you would like to copy to
* Hint: 1,2,10:13,20:24 means the configuration will be copy to port 1,2,10,11,12,13,20,21,23,24

Input multi port numbers in the "Port" column, and Port Type, Tagged VLAN ID, and untagged VLAN ID, and then click the **Set to Table** button to create VLAN ID configuration table.

# VLAN Management



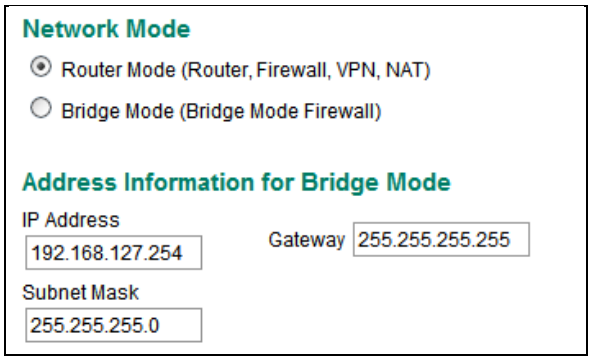
Use the **802.1Q VLAN Management** table to review the VLAN groups that were created, Joined Access Ports, Trunk Ports, and Hybrid Ports, and also Action for deleting VLANs which have no member ports in the list.

# Network Settings

## Mode Configuration (EDR-G902/G903 only)

### Network Mode

Each Industrial Secure Router provides **Router Mode** and **Bridge Mode** operation for different applications:




### Router Mode

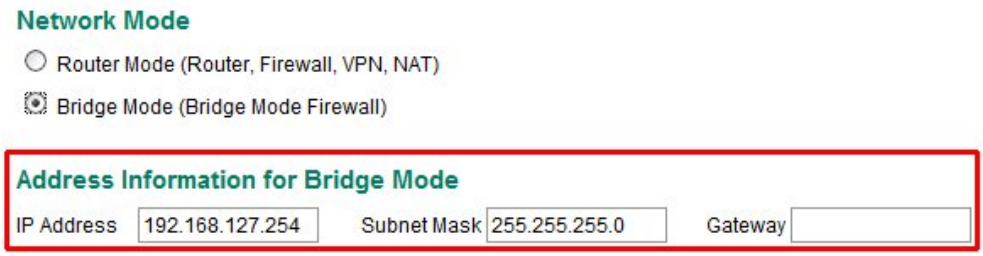
In this mode, the Industrial Secure Router operates as a gateway between different networks.

- Each interface (WAN1, WAN2, and LAN) has its own IP address and different subnets.
- Provides Routing, Firewall, VPN, and NAT functions.

### Bridge Mode

In this mode, the Industrial Secure Router operates as a Bridge mode firewall (or call transparent firewall) on a single subnet. Simply connect the Industrial Secure Router to an existing single subnet; you do not need to reconfigure the original subnet into different subnets and do not need to reconfigure the IP address of existing devices.

- The Industrial Secure Router only has one IP address, Network mask, and Gateway.
- VPN, NAT, WAN backup, VRRP, DHCP, and Dynamic DNS are not supported in this mode.




Select the appropriate operation mode and press **Activate** to change the mode of the Industrial Secure Router. After changing the operation mode, it may take 30 to 60 seconds to reboot system. If the webpage does not respond after 60 seconds, refresh webpage or press F5.

# WAN1 Configuration

**Connection**

Note that there are three different connection types for the WAN1 interface: Dynamic IP, Static IP, and PPPoE. A detailed explanation of the configuration settings for each type is given below.

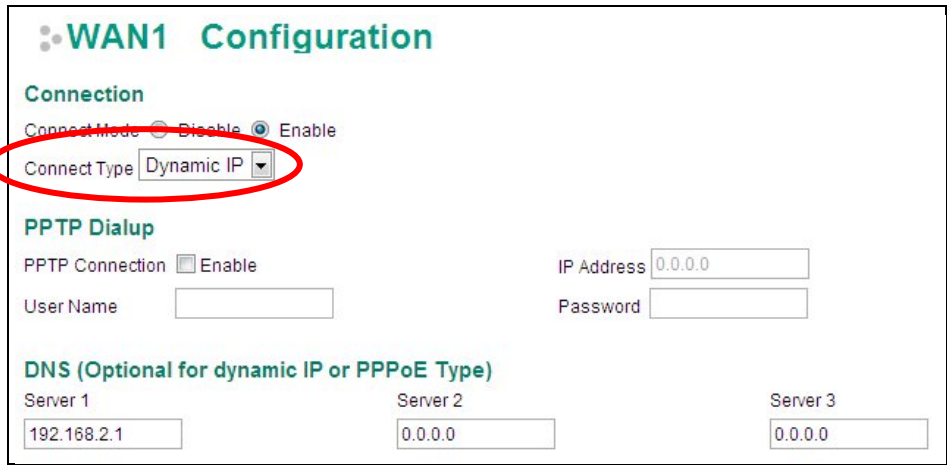
***Connection Mode***

| Setting | Description | Factory Default |
|---|---|---|
| Enable or Disable | Enable or Disable the WAN interface | Enable |

***Connection Type***

| Setting | Description | Factory Default |
|---|---|---|
| Static IP, Dynamic IP, PPPoE | Setup the connection type | Dynamic IP |

## Detailed Explanation of Dynamic IP Type




**PPTP Dialup**

Point-to-Point Tunneling Protocol is used for Virtual Private Networks (VPN). Remote users can use PPTP to connect to private networks from public networks.

***PPTP Connection***

| Setting | Description | Factory Default |
|---|---|---|
| Enable or Disable | Enable or Disable the PPTP connection | None |

***IP Address***

| Setting | Description | Factory Default |
|---|---|---|
| IP Address | The PPTP service IP address | None |

***User Name***

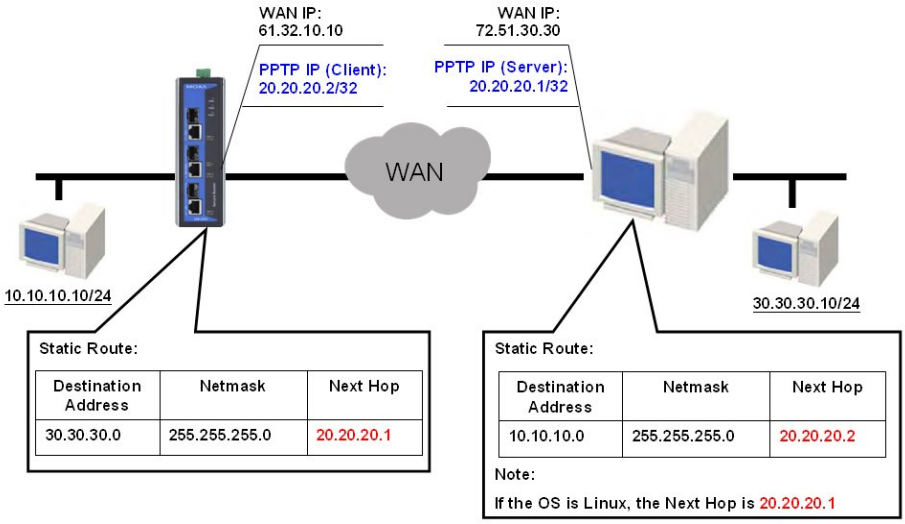
| Setting | Description | Factory Default |
|---|---|---|
| Max. 30 Characters | The Login username when dialing up to PPTP service | None |

***Password***

| Setting | Description | Factory Default |
|---|---|---|
| Max. 30 characters | The password for dialing the PPTP service | None |

**Example**

Suppose a remote user (IP: 10.10.10.10) wants to connect to the internal server (private IP: 30.30.30.10) via the PPTP protocol. The IP address for the PPTP server is 20.20.20.1. The necessary configuration settings are shown in the following figure.



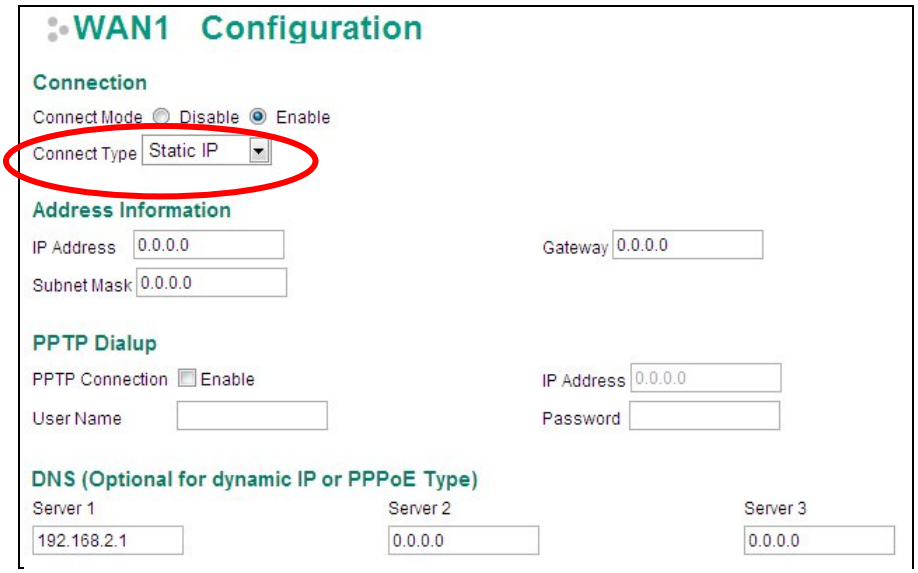

**DNS (Doman Name Server; optional setting for Dynamic IP and PPPoE types)**

***Server 1/2/3***

| Setting | Description | Factory Default |
|---|---|---|
| IP Address | The DNS IP address | None |

**NOTE** The priority of a manually configured DNS will be higher than the DNS from the PPPoE or DHCP server.

## Detailed Explanation of Static IP Type




**Address Information**

***IP Address***

| Setting | Description | Factory Default |
|---|---|---|
| IP Address | The interface IP address | None |

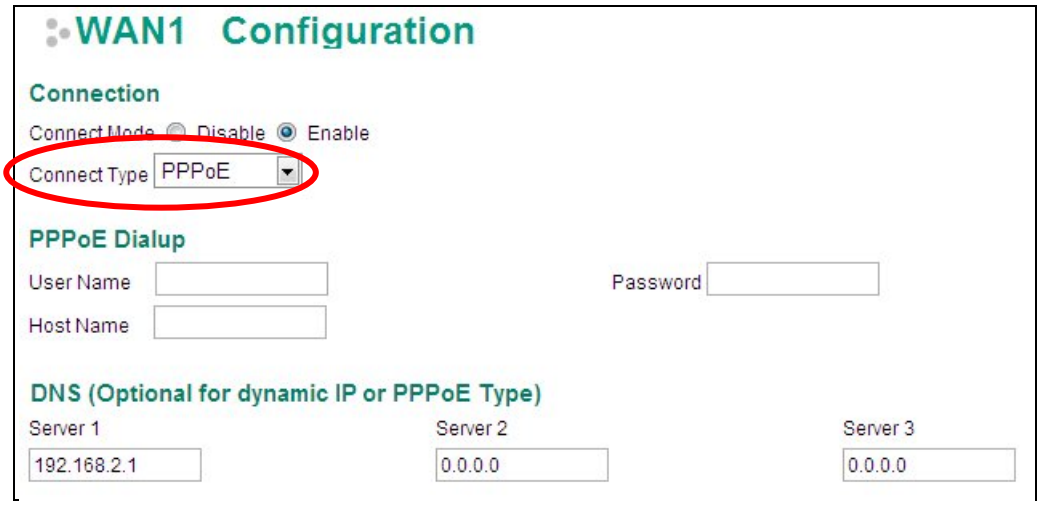
***Subnet Mask***

| Setting | Description | Factory Default |
|---|---|---|
| IP Address | The subnet mask | None |

***Gateway***

| Setting | Description | Factory Default |
|---|---|---|
| IP Address | The Gateway IP address | None |

### Detailed Explanation of PPPoE Type




**PPPoE Dialup**

***User Name***

| Setting | Description | Factory Default |
|---|---|---|
| Max. 30 characters | The User Name for logging in to the PPPoE server | None |

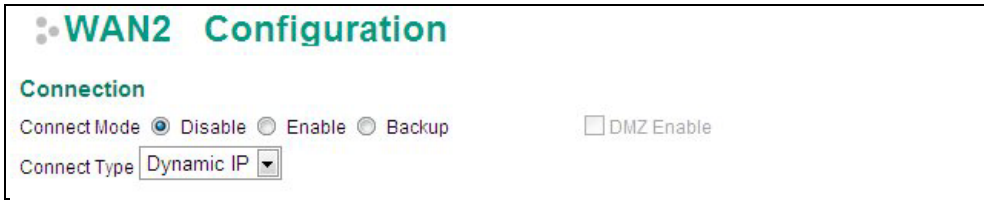
***Host Name***

| Setting | Description | Factory Default |
|---|---|---|
| Max. 30 characters | User-defined Host Name of this PPPoE server | None |

***Password***

| Setting | Description | Factory Default |
|---|---|---|
| Max. 30 characters | The login password for the PPPoE server | None |

## WAN2 Configuration (includes DMZ Enable, EDR-G903 only)




**Connection**

Note that there are there are three different connection types for the WAN2 interface: Dynamic IP, Static IP, and PPPoE. A detailed explanation of the configuration settings for each type is given below.

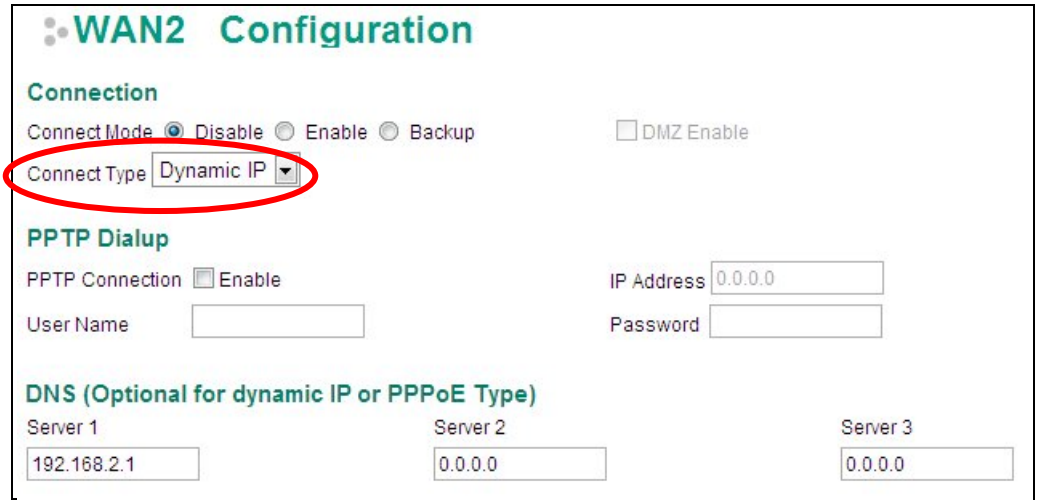
***Connection Mode***

| Setting | Description | Factory Default |
|---|---|---|
| Enable or Disable | Enable or Disable the WAN interface. | None |
| Backup | Enable WAN Backup mode | |
| DMZ | Enable DMZ mode (can only be enabled when the connection type is set to Static IP) | |

***Connection Type***

| Setting | Description | Factory Default |
|---|---|---|
| Static IP, Dynamic IP, PPPoE | Configure the connection type | Dynamic IP |

## Detailed Explanation of Dynamic IP Type




**PPTP Dialup**

Point-to-Point Tunneling Protocol is used for Virtual Private Networks (VPN). Remote users can use PPTP to connect to private networks from public networks.

***PPTP Connection***

| Setting | Description | Factory Default |
|---|---|---|
| Enable or Disable | Enable or Disable the PPTP connection | None |

***IP Address***

| Setting | Description | Factory Default |
|---|---|---|
| IP Address | The PPTP service IP address | None |

***User name***

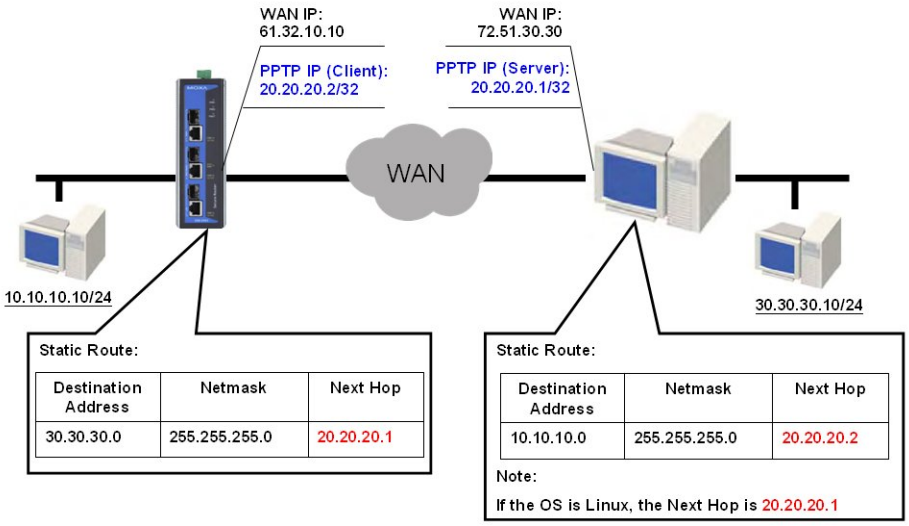
| Setting | Description | Factory Default |
|---|---|---|
| Max. 30 Characters | The Login username when dialing up to PPTP service | None |

***Password***

| Setting | Description | Factory Default |
|---|---|---|
| Max. 30 characters | The password for dialing the PPTP service | None |

**Example**

Suppose a remote user (IP: 10.10.10.10) wants to connect to the internal server (private IP: 30.30.30.10) via the PPTP protocol. The IP address for the PPTP server is 20.20.20.1. The necessary configuration settings are shown in the following figure.



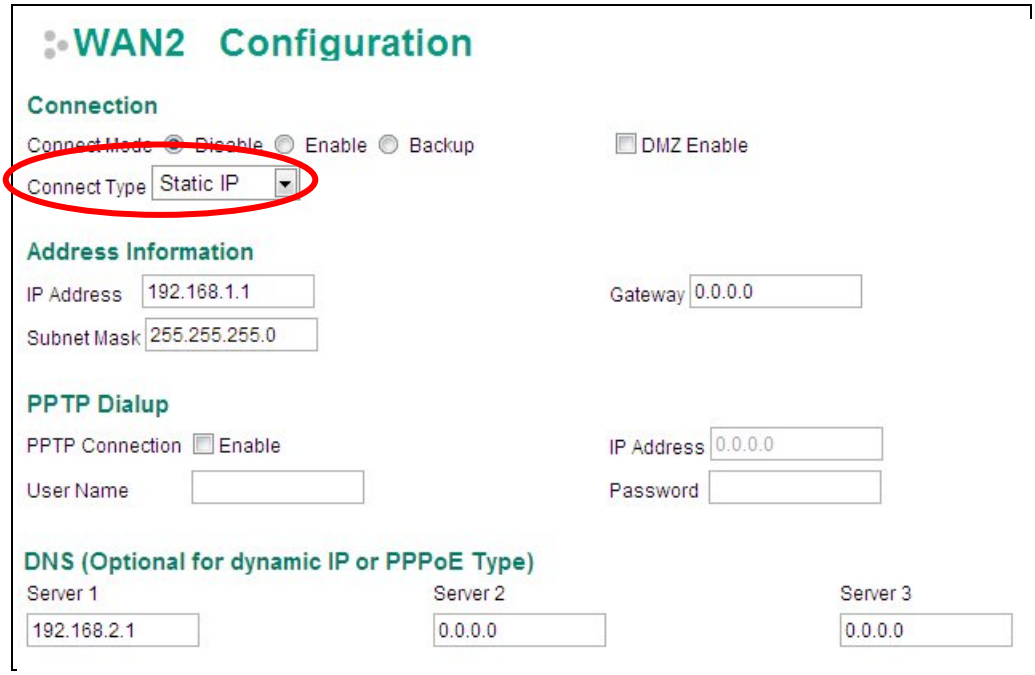

**DNS (Doman Name Server; optional setting for Dynamic IP and PPPoE types)**

***Server 1/2/3***

| Setting | Description | Factory Default |
|---|---|---|
| IP Address | The DNS IP Address | None |

**NOTE** The priority of a manually configured DNS will be higher than the DNS from the PPPoE or DHCP server.

## Detailed Explanation of Static IP Type




**Address Information**

***IP Address***

| Setting | Description | Factory Default |
|---|---|---|
| IP Address | The interface IP address | None |

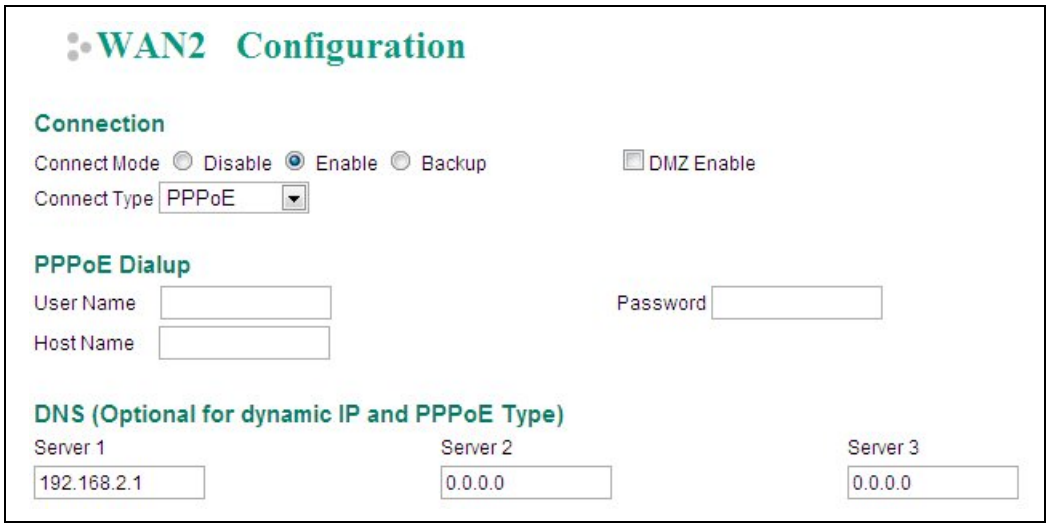
***Subnet Mask***

| Setting | Description | Factory Default |
|---|---|---|
| IP Address | The subnet mask | None |

***Gateway***

| Setting | Description | Factory Default |
|---|---|---|
| IP Address | The Gateway IP address | None |

### Detailed Explanation of PPPoE Type




**PPPoE Dialup**

***User Name***

| Setting | Description | Factory Default |
|---|---|---|
| Max. 30 characters | The User Name for logging in to the PPPoE server | None |

***Host Name***

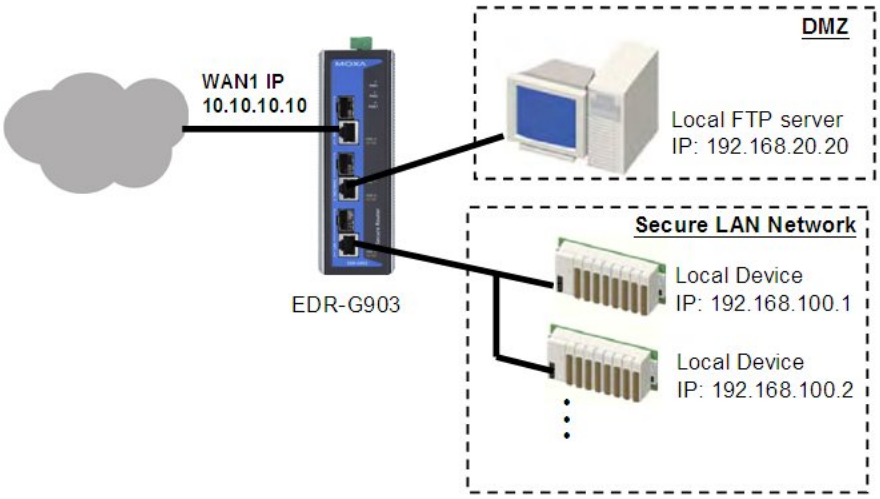
| Setting | Description | Factory Default |
|---|---|---|
| Max. 30 characters | User-defined host name for this PPPoE server | None |

***Password***

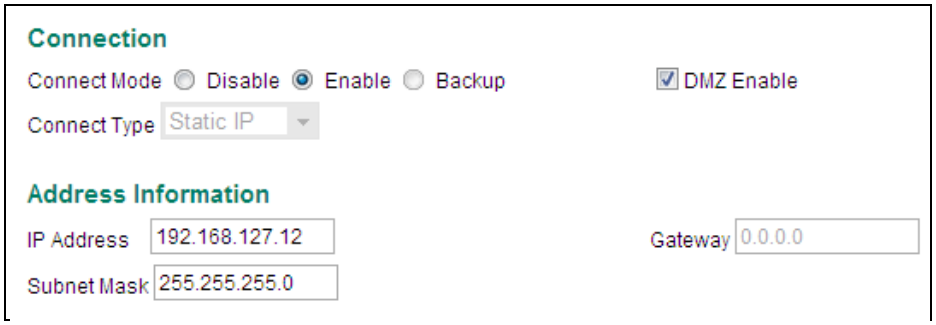
| Setting | Description | Factory Default |
|---|---|---|
| Max. 30 characters | The login password for this PPPoE server | None |

# Using DMZ Mode

A DMZ (demilitarized zone) is an isolated network for devices—such as data, FTP, web, and mail servers connected to a LAN network—that need to frequently connect with external networks. The deployment of an FTP server in a DMZ is illustrated in the following figure.



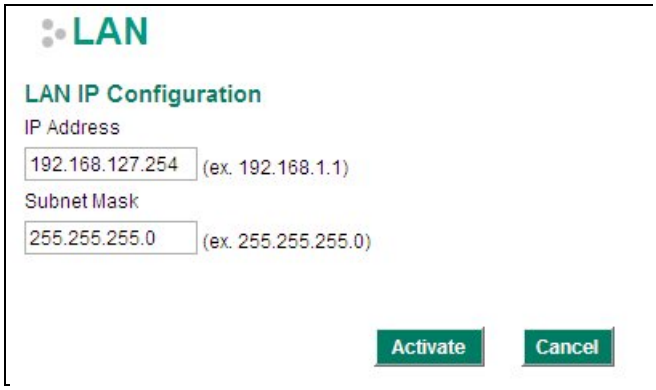
DMZ mode is configured on the **WAN2 configuration** web page. Set Connect Mode to Enable, Connect Type to Static IP, and checkmark the DMZ Enable check box. You will also need to input the IP Address and Subnet Mask. Click the **Activate** button to save the settings.




**NOTE** WAN2 configuration and DMZ mode are only available on EDR-G903

# LAN Interface (EDR-G902/G903)

A basic application of an industrial Firewall/VPN device is to provide protection when the device is connected to a LAN. In this regard, the LAN port connects to a secure (or trusted) area of the network, whereas the WAN1 and WAN2/DMZ ports connect to an insecure (or untrusted) area.




## LAN IP Configuration

***IP Address***

| Setting | Description | Factory Default |
|---|---|---|
| IP Address | The LAN interface IP address | 192.168.127.254 |

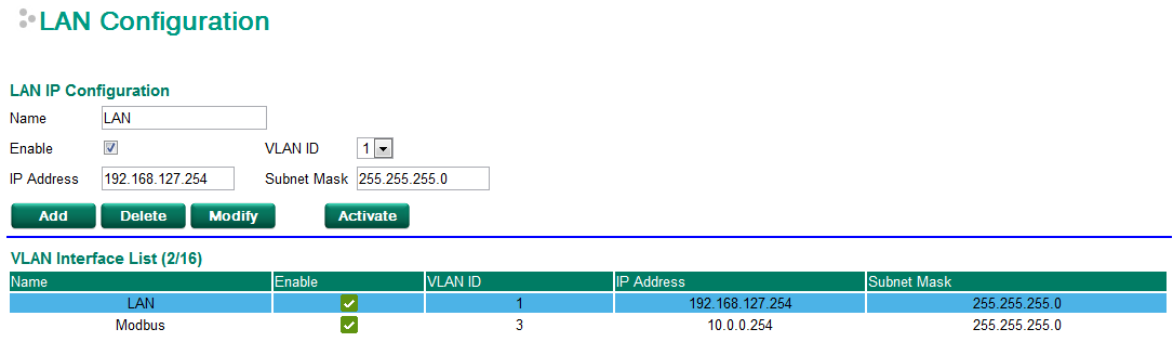
***Subnet Mask***

| Setting | Description | Factory Default |
|---|---|---|
| Subnet Mask | The subnet mask | 255.255.255.0 |

# LAN Configuration (EDR-810 series only)

The EDR-810 series supports up to 15 LAN interfaces for the 8 10/100 Mbps ports and the 2 Gigabit SFP ports. Use the **LAN Configuration** page to Add/Delete/Modify LAN interfaces.

## LAN Configuration




***Add a VLAN Interface***

Input a name of the VLAN interface, select a VLAN ID, and assign an IP address / Subnet Mask for the interface. Checkmark the **Enable** checkbox to enable this interface.

***Delete a VLAN Interface***

Select the item in the VLAN Interface List, and then click **Delete** to delete the item.

***Modify a VLAN Interface***

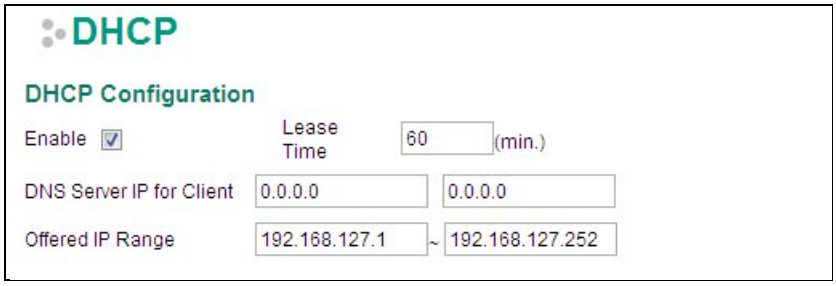
Select the item in the VLAN Interface List. Modify the attributes and then click **Modify** to change the configuration.

***Activate the VLAN Interface List***

After adding/deleting/modifying any VLAN interface, be sure to click **Activate**.

## DHCP Server

The Industrial Secure Router provides a DHCP (Dynamic Host Configuration Protocol) server function for LAN interfaces. When configured, the Industrial Secure Router will automatically assign an IP address to a Ethernet device from a defined IP range.




**DHCP configuration**

***DHCP Server Enable/Disable***

| Setting | Description | Factory Default |
|---|---|---|
| Enable or Disable | Enable or Disable DHCP server function | Enable |

***Lease Time***

| Setting | Description | Factory Default |
|---|---|---|
| ≥ 5 min. | The lease time of the DHCP server | 60 (min.) |

***DNS Server IP for Client***

| Setting | Description | Factory Default |
|---|---|---|
| IP Address | The DHCP server's IP address | None |

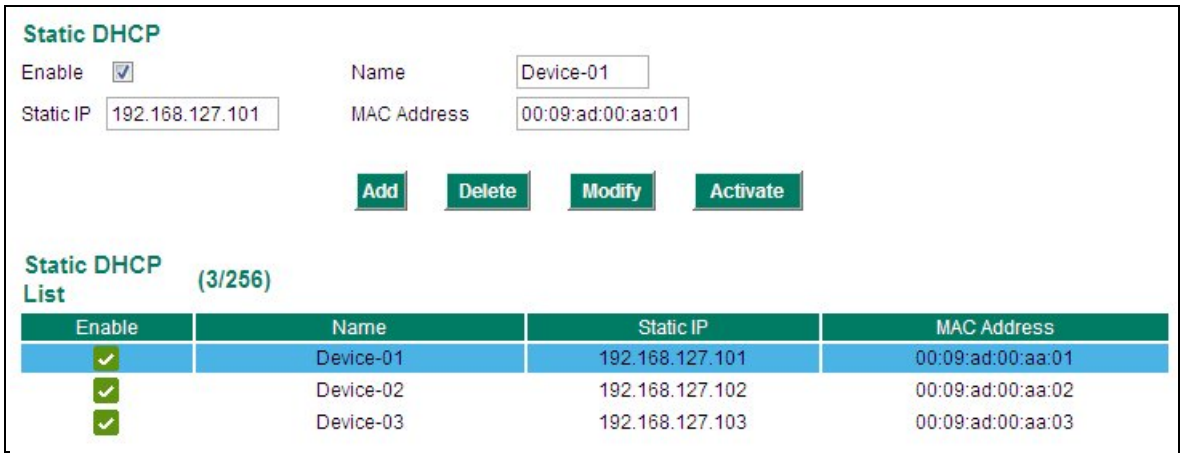
***Offered IP Range***

| Setting | Description | Factory Default |
|---|---|---|
| IP address | The offered IP address range for the DHCP server | 192.168.127.1 to 192.168.127.252 |

**NOTE**
1. The DHCP server is only available for LAN interfaces.
2. The Offered IP address range must be in the same Subnet on the LAN.

# Static DHCP List

Use the Static DHCP list to ensure that devices connected to the Industrial Secure Router always use the same IP address. The static DHCP list matches IP addresses to MAC addresses.




In the above example, a device named "Device-01" was added to the Static DHCP list, with static IP address set to 192.168.127.101 and MAC address set to 00:09:ad:00:aa:01. When a device with MAC address of 00:09:ad:00:aa:01 is connected to the Industrial Secure Router, the Industrial Secure Router will offer the IP address 192.168.127.101 to this device.

***Enable or Disable***

| Setting | Description | Factory Default |
|---|---|---|
| Enable or Disable | Enable or Disable the selected device in the Static DHCP List | Disabled |

***Name***

| Setting | Description | Factory Default |
|---|---|---|
| Max. 30 characters | The name of the selected device in the Static DHCP List | None |

***Static IP Address***

| Setting | Description | Factory Default |
|---|---|---|
| IP Address | The IP address of the selected device | None |

***MAC Address***

| Setting | Description | Factory Default |
|---|---|---|
| MAC Address | The MAC address of the selected device | None |

**Clickable Buttons**

***Add***

Use the Add button to input a new DHCP list. The Name, Static IP, and MAC address must be different than for the existing list.

***Delete***

Use the Delete button to delete the Static DHCP list. Click on a list to select it (the background color of the device will change to blue) and then click the Delete button.

***Modify***

To modify the information for a particular list, click on a list to select it (the background color of the device will change to blue), modify the information as needed using the check boxes and text input boxes near the top of the browser window, and then click Modify.

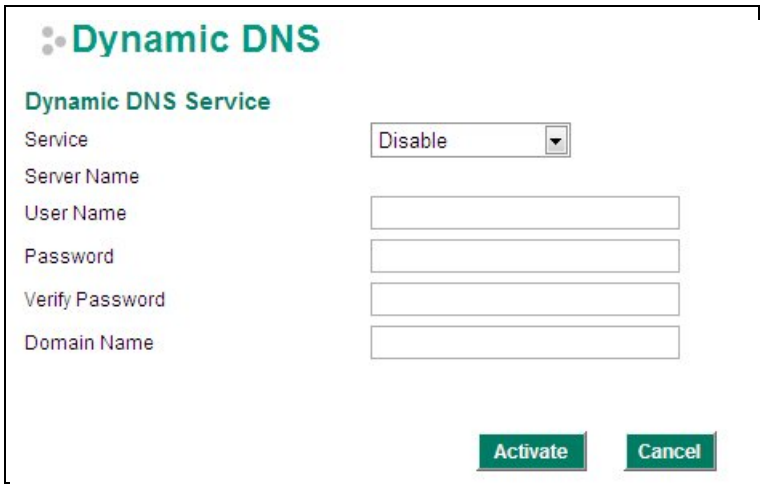
# DHCP Leased List

Use the DHCP Leased List to view the current DHCP clients.

| Name | MAC Address | IP Address | Time Left |
|---|---|---|---|
| Server | 00-0E-A6-09-7A-9E | 192.168.127.1 | 32m:36s |

# Dynamic DNS

Dynamic DNS (Domain Name Server) allows you to use a domain name (e.g., moxa.edr-g903) to connect to the Industrial Secure Router. The Industrial Secure Router can connect to 4 free DNS servers and register the user configurable Domain name in these servers.




***Service***

| Setting | Description | Factory Default |
|---|---|---|
| > Disable<br>> freedns.afraid.org<br>> www.3322.org<br>> members.dyndns.org<br>> dynupdate.no-ip.com | Disable or select the DNS server | Disable |

***User Name***

| Setting | Description | Factory Default |
|---|---|---|
| Max. 30 characters | The DNS server's user name | None |

***Password***

| Setting | Description | Factory Default |
|---|---|---|
| Max. 30 characters | The DNS server's password | None |

***Verify Password***

| Setting | Description | Factory Default |
|---|---|---|
| Max. 30 characters | Verifies the DNS server password | None |

***Domain name***

| Setting | Description | Factory Default |
|---|---|---|
| Max. 30 characters | The DNS server's domain name | None |

# Network Redundancy

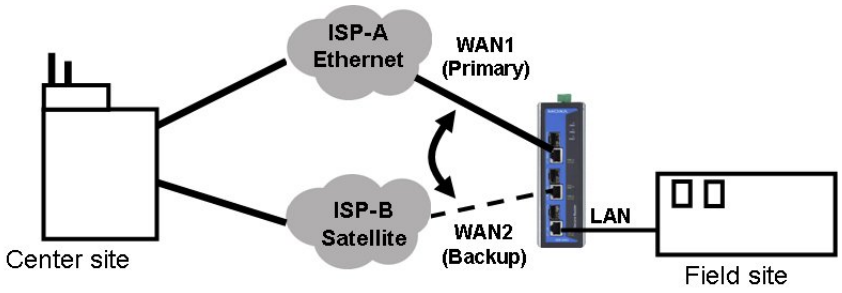
Moxa's Industrial Secure Router provides two types of network redundancy functions: WAN backup (EDR-G903 only) and VRRP. The Industrial Secure Router has two WAN interfaces: WAN1 is the primary WAN interface and WAN2 is the backup interface. When the Industrial Secure Router detects that connection WAN1 has failed (Link down or Ping fails), it will switch the communication path from WAN1 to WAN2 automatically. When WAN1 recovers, the major communication path will return to WAN1.

## WAN Backup (EDR-G903 only)

### How Dual WAN Backup Works

A power utility at a field site connects to a central office via two different ISPs (Internet Service Providers). ISP-A uses Ethernet and ISP-B uses satellite for data transmission, with Ethernet used as the major connection and the satellite as the backup connection. This makes sense since the cost of transmitting through the satellite is greater than the cost of transmitting over the Ethernet. Traditional solutions would use two routers to connect to the different ISPs. In this case, if the connection to the primary ISP fails, the connection must be switched to the backup ISP manually.

The Industrial Secure Router's WAN backup function checks the link status and the connection integrity between the Industrial Secure Router and the ISP or central office. When the primary WAN interface fails, it will switch to the backup WAN automatically to keep the connection alive.

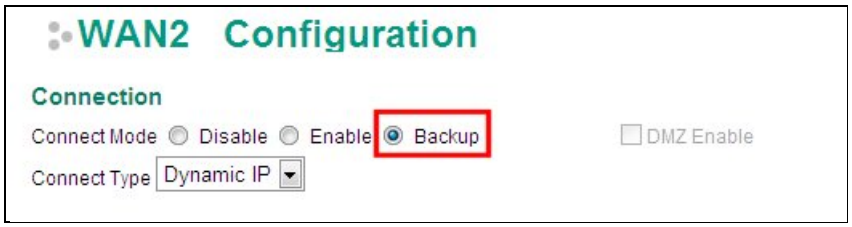



When configuring the Industrial Secure Router, choose one of the two following conditions to activate the backup path:

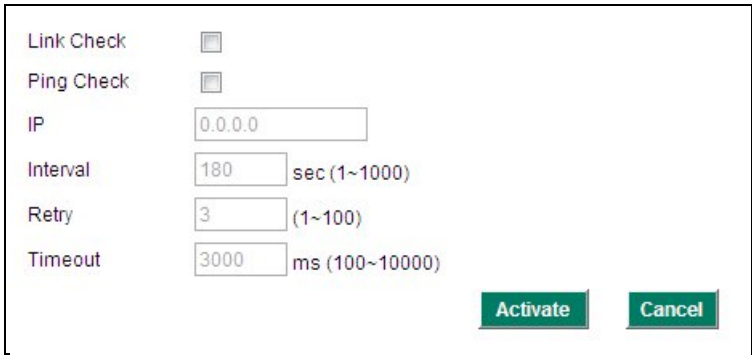
- Link Check: WAN1 link down
- Ping Check: Sends ping commands to a specific IP address (e.g., the IP address of the ISP's server) from WAN1 based on user configurable Time Interval, Retry, and Timeout.

When the WAN backup function is enabled and the Link Check or Ping Check for the WAN1 interface fails, the backup interface (WAN2) will be enabled as the primary interface.

## WAN Backup Configuration




Select Backup for the WAN2/DMZ Connect Mode, and then go to the **Network Redundancy → WAN Backup** setting page for the WAN Backup configuration.




***Link Check***

| Setting | Description | Factory Default |
|---|---|---|
| Enable or Disable | Activate Backup function by checking the link status of WAN1 | Disabled |

***Ping Check***

| Setting | Description | Factory Default |
|---|---|---|
| Enable or Disable | Activates the Backup function if unable to ping from the Industrial Secure Router to a specified IP address. | Disabled |

***IP***

| Setting | Description | Factory Default |
|---|---|---|
| IP address | The Industrial Secure Router will check the ping integrity of this IP Address if the Ping Check function is Enabled | None |

**NOTE** The IP address for Ping Check function should be on the network segment of WAN1.

***Interval***

| Setting | Description | Factory Default |
|---|---|---|
| 1 to 1000 sec | Users can set up a different Ping Interval for a different network topology. | 180 sec. |

***Retry***

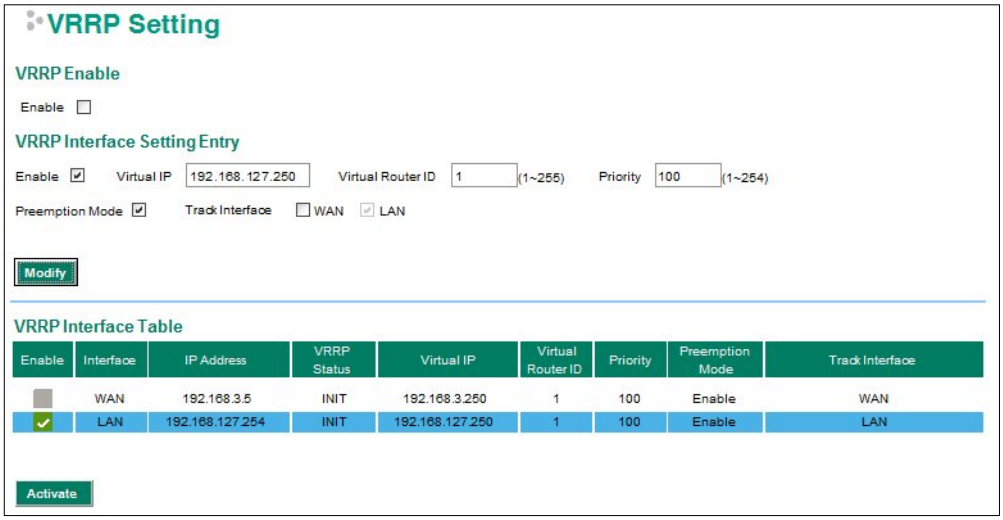
| Setting | Description | Factory Default |
|---|---|---|
| 1 to 100 | Users can configure the number of retries. If the number of continuous retries exceeds this number, the Industrial Secure Router will activate the backup path. | 3 |

***Timeout***

| Setting | Description | Factory Default |
|---|---|---|
| 100 to 10000 (ms) | The timeout criterion of Ping Check | 3000 ms |

# Virtual Router Redundancy Protocol (VRRP)

## VRRP Settings




Virtual Router Redundancy Protocol (VRRP) can solve the problem with static configuration. VRRP enables a group of routers to form a single virtual router with a virtual IP address. The LAN clients can then be configured with the virtual router's virtual IP address as their default gateway. The virtual router is the combination of a group of routers, and is also known as a VRRP group.

***Enable***

| Setting | Description | Factory Default |
|---|---|---|
| Enable | Enables VRRP | Disable |

***VRRP Interface Setting Entry***

| Setting | Description | Factory Default |
|---|---|---|
| Enable | Enables VRRP entry | Disabled |
| Virtual IP | L3 switches / routers in the same VRRP group must be set to the same virtual IP address as the VRRP ID. This virtual IP address must belong to the same address range as the real IP address of the interface. | 0.0.0.0 |
| Virtual Router ID | Virtual Router ID is used to assign a VRRP group. The L3 switches / routers, which operate as master / backup, should have the same ID. Moxa L3 switches / routers support one virtual router ID for each interface. IDs can range from 1 to 255. | 0 |
| Priority | Determines priority in a VRRP group. The priority value range is 1 to 255 and the 255 is the highest priority. If several L3 switches / routers have the same priority, the router with higher IP address has the higher priority. The usable range is "1 to 255". | 100 |
| Preemption Mode | Determines whether a backup L3 switch / router will take the authority of master or not. | Enabled |
| Track Interface | The Track Interface is used to track specific interface within the router that can change the status of the virtual router for a VRRP Group. For example, the WAN interface can be tracked and if the link is down, the other backup router will become the new master of the VRRP group. | Disable |

# Static Routing and Dynamic Routing

The Industrial Secure Router supports two routing methods: static routing and dynamic routing. Dynamic routing makes use of RIP V1/V1c/V2. You can either choose one routing method, or combine the two methods to establish your routing table. A routing entry includes the following items: the destination address, the next hop address (which is the next router along the path to the destination address), and a metric that represents the cost we have to pay to access a different network.

### Static Route

You can define the routes yourself by specifying what is the next hop (or router) that the Industrial Secure Router forwards data for a specific subnet. The settings of the Static Route will be added to the routing table and stored in the Industrial Secure Router.

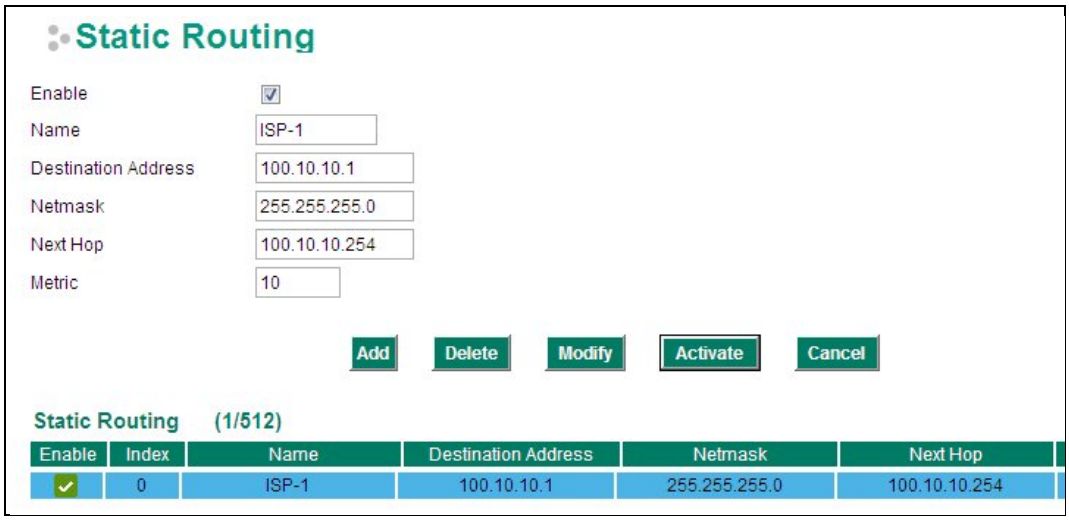
### RIP (Routing Information Protocol)

RIP is a distance vector-based routing protocol that can be used to automatically build up a routing table in the Industrial Secure Router.

The Industrial Secure Router can efficiently update and maintain the routing table, and optimize the routing by identifying the smallest metric and most matched mask prefix.

# Static Routing

The Static Routing page is used to configure the Industrial Secure Router's static routing table.




***Enable***

Click the checkbox to enable Static Routing.

***Name***

The name of this Static Router list

***Destination Address***

You can specify the destination IP address.

***Netmask***

This option is used to specify the subnet mask for this IP address.

***Next Hop***

This option is used to specify the next router along the path to the destination.

***Metric***

Use this option to specify a "cost" for accessing the neighboring network.

**Clickable Buttons**

***Add***

For adding an entry to the Static Routing Table.

***Delete***

For removing selected entries from the Static Routing Table.

***Modify***

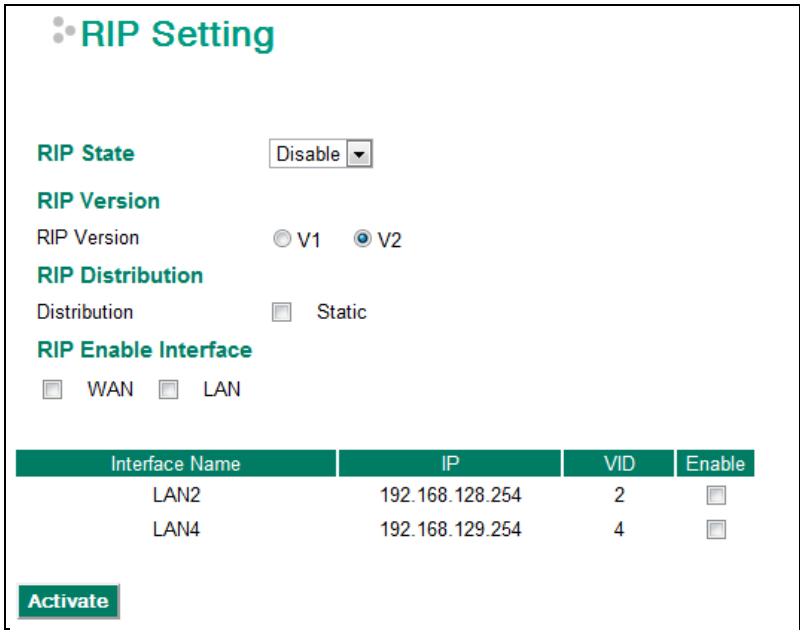
For modifying the content of a selected entry in the Static Routing Table.

**NOTE** The entries in the Static Routing Table will not be added to the Industrial Secure Router's routing table until you click the Activate button.

# RIP (Routing Information Protocol)

RIP is a distance-vector routing protocol that employs the hop count as a routing metric. RIP prevents routing from looping by implementing a limit on the number of hops allowed in a path from the source to a destination.

The RIP **Setting** page is used to set up the RIP parameters.




***RIP State***

| Setting | Description | Factory Default |
|---|---|---|
| Enable/Disable | Enable or Disable RIP protocol | Disable |

***RIP Version***

| Setting | Description | Factory Default |
|---|---|---|
| V1/V2 | Select RIP protocol version. | V2 |

***RIP Distribution***

| Setting | Description | Factory Default |
|---|---|---|
| Static | Check the checkbox to enable the Redistributed Static Route function. The entries that are set in a static route will be re-distributed if this option is enabled. | Unchecked |

***RIP Enable Interface***

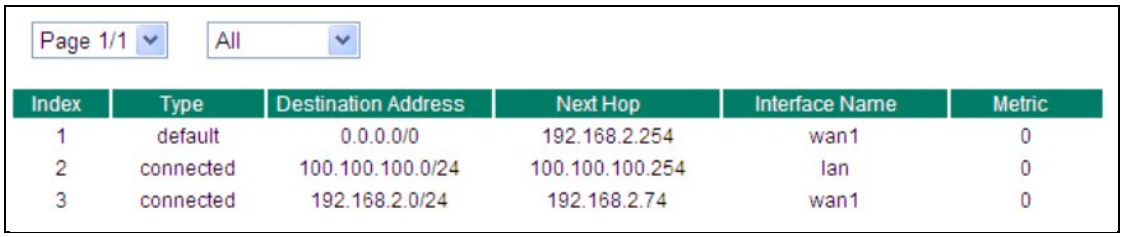
| Setting | Description | Factory Default |
|---|---|---|
| WAN | Check the checkbox to enable RIP in the WAN interface. | Unchecked |
| LAN | Check the checkbox to enable RIP in the LAN interface. | |

***RIP Interface Table (EDR-810 series only)***

| Setting | Description | Factory Default |
|---|---|---|
| Enable/Disable | Check the checkbox to enable RIP for each interface. | Unchecked |

## Routing Table

The **Routing Table** page shows all routing entries.




***All Routing Entry List***

| Setting | Description | Factory Default |
|---|---|---|
| All | Show all routing entries | N/A |
| Connected | Show connected routing entries | N/A |
| Static | Show Static routing entries | N/A |
| RIP | Show RIP routing entries | N/A |
| Others | Show others routing entries | N/A |

# Network Address Translation (NAT)

## NAT Concept

NAT (Network Address Translation) is a common security function for changing the IP address during Ethernet packet transmission. When the user wants to hide the internal IP address (LAN) from the external network (WAN), the NAT function will translate the internal IP address to a specific IP address, or an internal IP address range to one external IP address. The benefits of using NAT include:

- Uses the N-1 or Port forwarding Nat function to hide the Internal IP address of a critical network or device to increase the level of security of industrial network applications.
- Uses the same private IP address for different, but identical, groups of Ethernet devices. For example, 1-to-1 NAT makes it easy to duplicate or extend identical production lines.

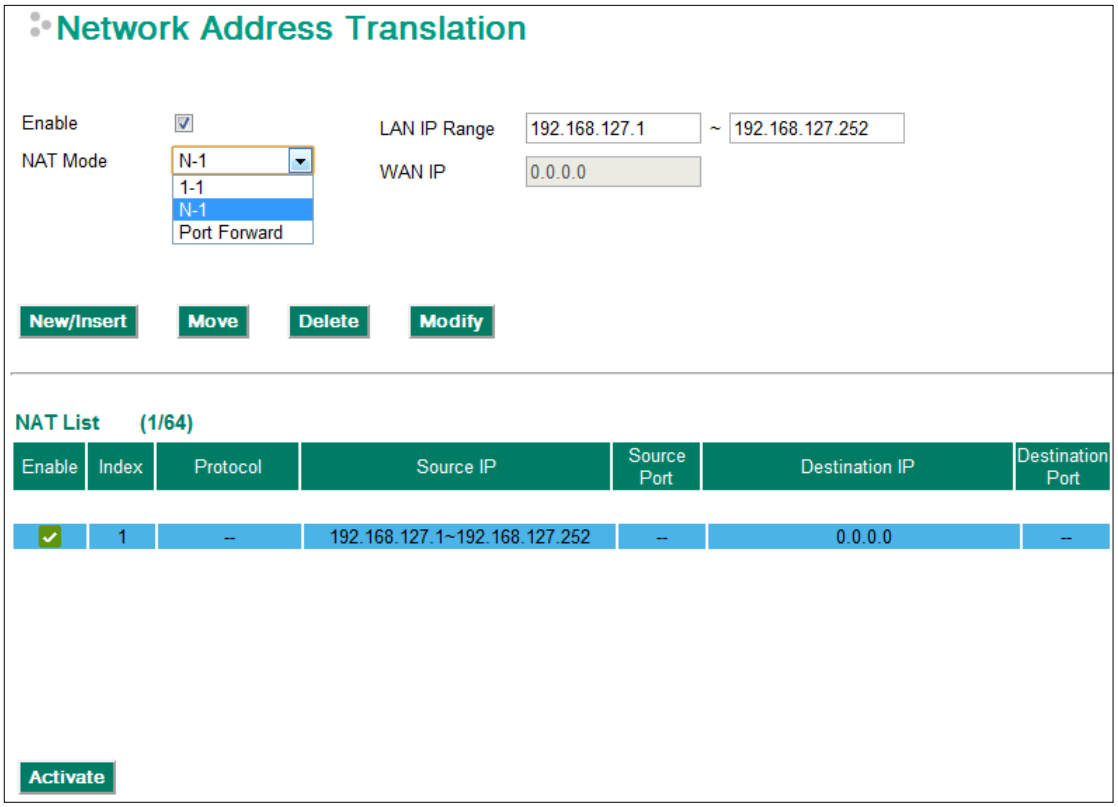
**NOTE** The NAT function will check if incoming or outgoing packets match the policy. It starts by checking the packet with the first policy (Index=1); if the packet matches this policy, the Industrial Secure Router will translate the address immediately and then start checking the next packet. If the packet does not match this policy, it will check with the next policy.

**NOTE** The maximum number of NAT policies for the Industrial Secure Router is 128.

## N-to-1 NAT

If the user wants to hide the Internal IP address from users outside the LAN, the easiest way is to use the N-to-1 (or N-1) NAT function. The N-1 NAT function replaces the source IP Address with an external IP address, and adds a logical port number to identify the connection of this internal/external IP address. This function is also called "Network Address Port Translation" (NAPT) or "IP Masquerading."

The N-1 NAT function is a one-way connection from an internal secure area to an external non-secure area. The user can initialize the connection from the internal to the external network, but may not be able to initialize the connection from the external to the internal network.




***Enable/Disable NAT Policy***

| Setting | Description | Factory Default |
|---|---|---|
| Enable or Disable | Enable or disable the selected NAT policy | Enabled |

***NAT Mode***

| Setting | Description | Factory Default |
|---|---|---|
| N-1<br>1-1<br>Port Forwarding | Select the NAT types | N-1 |

***Interface (N-1 mode)***

| Setting | Description | Factory Default |
|---|---|---|
| Auto<br>WAN1<br>WAN2 | Select the Interface for this NAT Policy | Auto |

The Industrial Secure Router provides a Dual WAN backup function for network redundancy. If the interface is set to Auto, the NAT Mode is set to N-1, and the WAN backup function is enabled, the primary WAN interface is WAN1. If the WAN1 connection fails, the WAN interface of this N-1 policy will apply to WAN2 and switch to WAN2 for N-1 outgoing traffic until the WAN1 interface recovers.

***IP Range***

| Setting | Description | Factory Default |
|---|---|---|
| IP address | Select the Internal IP range for IP translation to WAN IP address | None |

***WAN IP (N-1 mode)***

| Setting | Description | Factory Default |
|---|---|---|
| IP address | The IP address of the user selected interface (WAN1, WAN2, and Auto) in this N-to-1 policy. | None |

***Add a NAT Rule***

Checked the "Enable" checkbox and input the correspondent NAT parameters in the page, and then click "New/Insert" to add it into the NAT List Table. Finally, click "Activate" to activate the configuration.

***Delete a NAT Rule***

Select the item in the NAT List Table, then, click "Delete" to delete the item.

***Modify a NAT Rule***

Select the item in the NAT List Table. Modify the attributes and click "Modify" to change the configuration.

***Activate NAT List Table***

After adding/deleting/modifying any NAT Rules, be sure to Activate it.

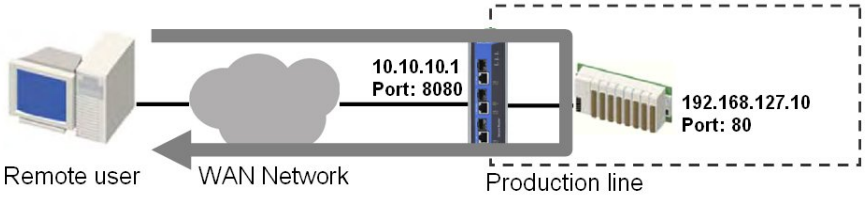
**NOTE** The Industrial Secure Router will add an N-1 policy from the source IP, 192.168.127.1 to 192.168.127.252 to the WAN1 interface after activating the Factory Default.

# Port Forwarding (NAT Mode option)

If the initial connection is from outside the LAN, but the user still wants to hide the Internal IP address, one way to do this is to use the Port Forwarding NAT function.

The user can specify the port number of an external IP address (WAN1 or WAN2) in the Port Forwarding policy list. For example, if the IP address of a web server in the internal network is 192.168.127.10 with port 80, the user can set up a port forwarding policy to let remote users connect to the internal web server from external IP address 10.10.10.10 through port 8080. The Industrial Secure Router will transfer the packet to IP address 192.168.127.10 through port 80.

The Port Forwarding NAT function is one way of connecting from an external insecure area (WAN) to an internal secure area (LAN). The user can initiate the connection from the external network to the internal network, but will not able to initiate a connection from the internal network to the external network.



***Enable/Disable NAT policy***

| Setting | Description | Factory Default |
|---|---|---|
| Enable or Disable | Enable or disable the selected NAT policy | Enabled |

***NAT Mode***

| Setting | Description | Factory Default |
|---|---|---|
| N-1<br>1-1<br>Port Forward | Select the NAT types | N-1 |

***Interface (Port Forward mode)***

| Setting | Description | Factory Default |
|---|---|---|
| WAN1<br>WAN2 | Select the Interface for this NAT Policy | WAN1 |

***Protocol (Port Forward mode)***

| Setting | Description | Factory Default |
|---|---|---|
| TCP<br>UDP<br>TCP & UDP | Select the Protocol for NAT Policy | TCP |

***WAN Port (Port Forward mode)***

| Setting | Description | Factory Default |
|---|---|---|
| 1 to 65535 | Select a specific WAN port number | None |

***LAN/DMZ IP (Port Forward mode)***

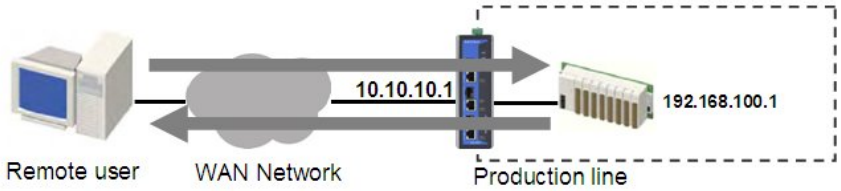
| Setting | Description | Factory Default |
|---|---|---|
| IP Address | The translated IP address in the internal network | None |

***LAN/DMZ Port (Port Forward mode)***

| Setting | Description | Factory Default |
|---|---|---|
| 1 to 65535 | The translated port number in the internal network | None |

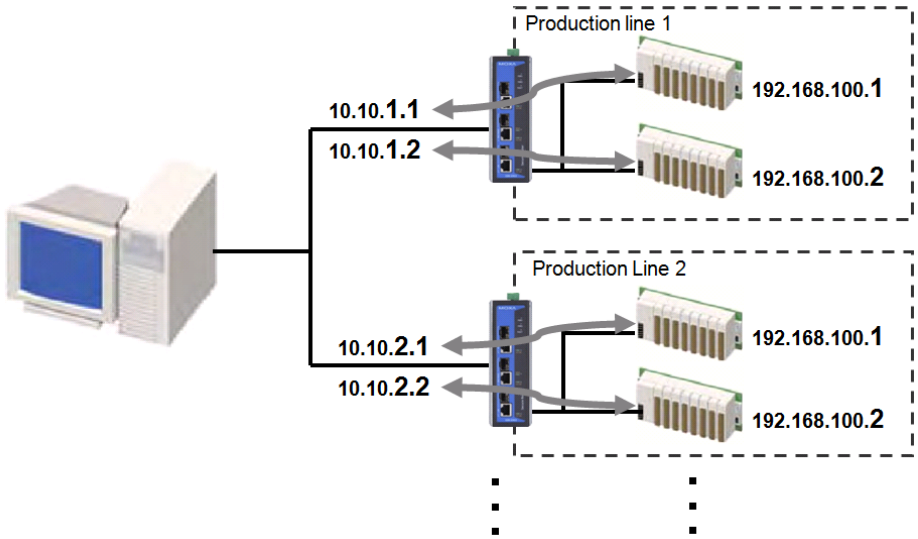
# 1-to-1 NAT

If the internal device and external device need to communicate with each other, choose 1-to-1 NAT, which offers bi-directional communication (N-to-1 and Port forwarding are both single-directional communication NAT functions).




1-to-1 NAT is usually used when you have a group of internal servers with private IP addresses that must connect to the external network. You can use 1-to-1 NAT to map the internal servers to public IP addresses. The IP address of the internal device will not change.

The figure below illustrates how a user could extend production lines, and use the same private IP addresses of internal devices in each production line. The internal private IP addresses of these devices will map to different public IP addresses. Configuring a group of devices for 1-to-1 NAT is easy and straightforward.



**1-to-1 NAT Setting for EDR-G903 in Production Line 1**

NAT List (2/64)

| Enable | Index | Protocol | Source IP | Source Port | Destination IP |
|---|---|---|---|---|---|
| ☑ | 1 | -- | 192.168.100.1 | -- | 10.10.1.1 |
| ☑ | 2 | -- | 192.168.100.2 | -- | 10.10.1.2 |

**1-to-1 NAT Setting for EDR-G903 in Production Line 2**

NAT List (2/64)

| Enable | Index | Protocol | Source IP | Source Port | Destination IP |
|---|---|---|---|---|---|
| ☑ | 1 | -- | 192.168.100.1 | -- | 10.10.2.1 |
| ☑ | 2 | -- | 192.168.100.2 | -- | 10.10.2.2 |

***Enable/Disable NAT policy***

| Setting | Description | Factory Default |
|---|---|---|
| Enable or Disable | Enable or disable the selected NAT policy | None |

***NAT Mode***

| Setting | Description | Factory Default |
|---|---|---|
| N-1<br>1-1<br>Port Forward | Select the NAT types | None |

***Interface (1-1 NAT type)***

| Setting | Description | Factory Default |
|---|---|---|
| WAN1<br>WAN2 | Select the Interface for this NAT Policy | WAN1 |

***LAN/DMZ IP (1-1 NAT type)***

| Setting | Description | Factory Default |
|---|---|---|
| IP Address | Select the Internal IP address in LAN/DMZ network area | None |

***WAN IP (1-1 NAT type)***

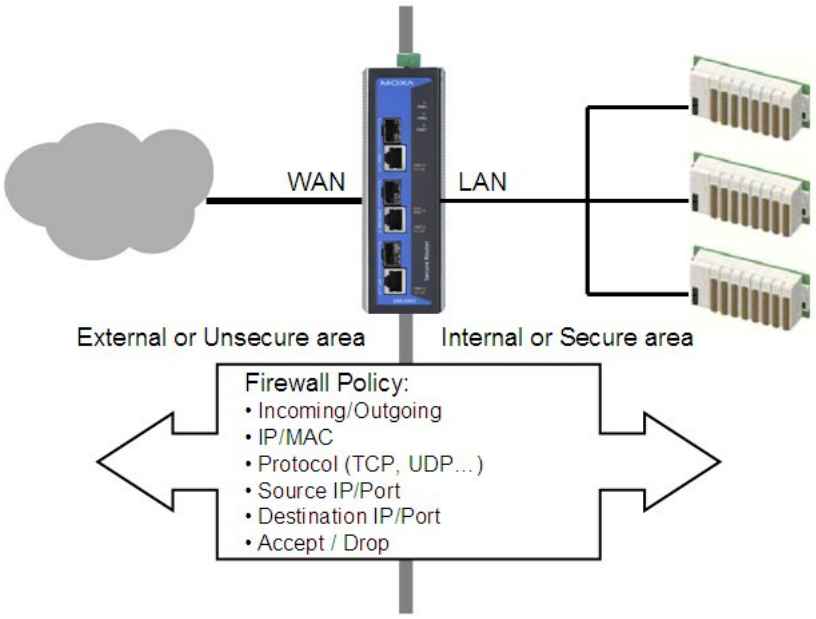
| Setting | Description | Factory Default |
|---|---|---|
| IP Address | Select the external IP address in WAN network area | None |

**NOTE** The Industrial Secure Router can obtain an IP address via DHCP or PPPoE. However, if this dynamic IP address is the same as the WAN IP for 1-to-1 NAT, then the 1-to-1 NAT function will not work. For this reason, we recommend disabling the DHCP/PPPoE function when using the 1-to-1 NAT function.

# Firewall Settings

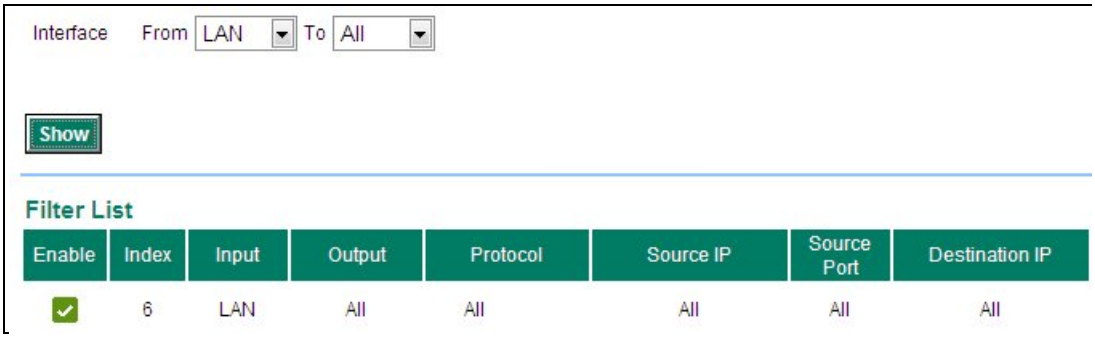
## Firewall Policy Concept

A firewall device is commonly used to provide secure traffic control over an Ethernet network, as illustrated in the following figure. Firewall devices are deployed at critical points between an external network (the non-secure part) and an internal network (the secure part).




## Firewall Policy Overview

The Industrial Secure Router provides a Firewall Policy Overview that lists firewall policies by interface direction.




Select the **From** interface and **To** interface and then click the **Show** button. The Policy list table will show the policies that match the **From-To** interface.

***Interface From/To***

| Setting | Description | Factory Default |
|---|---|---|
| All (WAN1/WAN2/LAN) | Select the From Interface and To interface | From All to All |
| WAN1 | | |
| WAN2 | | |
| LAN | | |

# Firewall Policy Configuration

The Industrial Secure Router's Firewall policy provides secure traffic control, allowing users to control network traffic based on the following parameters.

***Enable***

| Setting | Description | Factory Default |
|---|---|---|
| Enable or Disable | Enable or disable the selected Firewall policy | Enabled |

***Interface From/To***

| Setting | Description | Factory Default |
|---|---|---|
| All (WAN1/WAN2/LAN) | Select the From Interface and To interface | From All to All |
| WAN1 | | |
| WAN2 | | |
| LAN | | |

***Quick Automation Profile***

| Setting | Description | Factory Default |
|---|---|---|
| Refer to the "Quick Automation Profile" section. | Select the Protocol parameters in this Firewall Policy | None |

***Service***

| Setting | Description | Factory Default |
|---|---|---|
| IP Filter | This Firewall policy will filter by IP address | IP Filter |
| MAC Filter | This Firewall policy will filter by MAC address | |

***Target***

| Setting | Description | Factory Default |
|---|---|---|
| Accept | The packet will penetrate the firewall when it matches this firewall policy | Accept |
| Drop | The packet will not penetrate the firewall when it matches this firewall policy | |

***Source IP***

| Setting | Description | Factory Default |
|---|---|---|
| All (IP Address) | This Firewall Policy will check all Source IP addresses in the packet | All |
| Single (IP Address) | This Firewall Policy will check single Source IP addresses in the packet | |
| Range (IP Address) | This Firewall Policy will check multiple Source IP addresses in the packet | |

***Source Port***

| Setting | Description | Factory Default |
|---|---|---|
| All (Port number) | This Firewall Policy will check all Source port numbers in the packet | All |
| Single (Port number) | This Firewall Policy will check single Source Port numbers in the packet | |
| Range (Port number) | This Firewall Policy will check multiple Source port numbers in the packet | |

***Destination IP***

| Setting | Description | Factory Default |
|---|---|---|
| All (IP Address) | This Firewall Policy will check all Destination IP addresses in the packet | All |
| Single (IP Address) | This Firewall Policy will check single Destination IP addresses in the packet | |
| Range (IP Address) | This Firewall Policy will check multiple Destination IP addresses in the packet | |

***Destination Port***

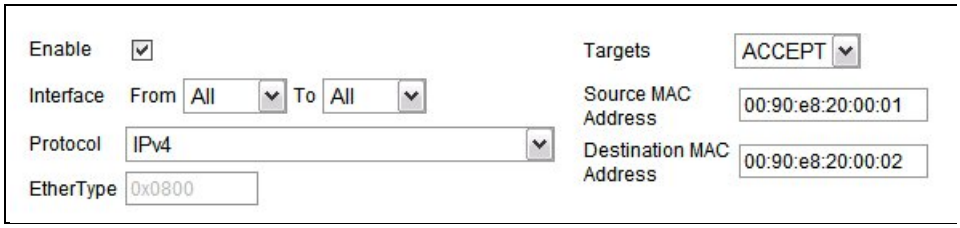
| Setting | Description | Factory Default |
|---|---|---|
| All (Port number) | This Firewall Policy will check all Destination port numbers in the packet | All |
| Single (Port number) | This Firewall Policy will check single Destination Port numbers in the packet | |
| Range (Port number) | This Firewall Policy will check multiple Destination port numbers in the packet | |

**NOTE** The Industrial Secure Router's firewall function will check if incoming or outgoing packets match the firewall policy. It starts by checking the packet with the first policy (Index=1); if the packet matches this policy, it will accept or drop the packet immediately and then check the next packet. If the packet does not match this policy it will check with the next policy.

**NOTE** The maximum number of Firewall policies for the Industrial Secure Router is 256.

# Layer 2 Policy Setup (Only in Bridge Mode for EDR-G902/G903)

When the Industrial Secure Router is in Bridge Mode (referring to section of Mode Configuration in Network Settings), it provides an advanced Layer 2 firewall policy for secure traffic control, which depends on the following parameters:



***Interface From/To***

| Setting | Description | Factory Default |
|---|---|---|
| All (WAN1/WAN2/LAN) | Select the From Interface and To interface | None |
| WAN1 | | |
| WAN2 | | |
| LAN | | |

***Protocol***

| Setting | Description | Factory Default |
|---|---|---|
| Refer to table "EtherType for Layer 2 Protocol" for a more detailed description | Select the Layer 2 Protocol in this Firewall Policy | None |

***EtherType***

| Setting | Description | Factory Default |
|---|---|---|
| 0x0600 to 0xFFFF | When Protocol is set to "Manual" you can set up EtherType manually | None |

***Target***

| Setting | Description | Factory Default |
|---|---|---|
| Accept | The packet will pass the Firewall when it matches this Firewall policy | None |
| Drop | The packet will not pass the Firewall when it matches this Firewall policy | None |

***Source MAC Address***

| Setting | Description | Factory Default |
|---|---|---|
| Mac Address | This Firewall Policy will check all Source MAC addresses of the packet | 00:00:00:00:00:00 |

***Destination MAC Address***

| Setting | Description | Factory Default |
|---|---|---|
| Mac Address | This Firewall Policy will check all destination MAC addresses of the packet | 00:00:00:00:00:00 |

The following table shows the Layer 2 protocol types commonly used in Ethernet frames.

***EtherType for Layer 2 Protocol***

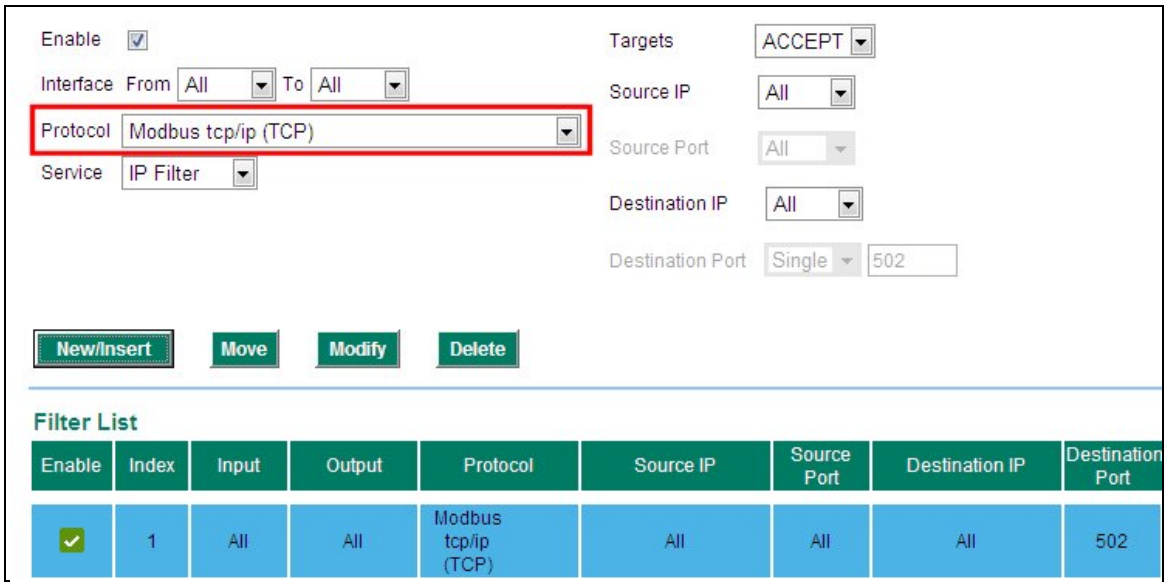
| Type | Layer 2 Protocol |
|---|---|
| 0x0800 | IPv4 (Internet Protocol version 4) |
| 0x0805 | X.25 |
| 0x0806 | ARP (Address Resolution Protocol) |
| 0x0808 | Frame Relay ARP |
| 0x08FF | G8BPQ AX.25 Ethernet Packet |
| 0x6000 | DEC Assigned proto |
| 0x6001 | DEC DNA Dump/Load |
| 0x6002 | DEC DNA Remote Console |
| 0x6003 | DEC DNA Routing |
| 0x6004 | DEC LAT |
| 0x6005 | DEC Diagnostics |
| 0x6006 | DEC Customer use |
| 0x6007 | DEC Systems Comms Arch |
| 0x6558 | Trans Ether Bridging |
| 0x6559 | Raw Frame Relay |
| 0x80F3 | Appletalk AARP |

| | |
|---|---|
| 0x809B | Appletalk |
| 0x8100 | 8021Q VLAN tagged frame |
| 0x8137 | Novell IPX |
| 0x8191 | NetBEUI |
| 0x86DD | IPv6 (Internet Protocol version 6) |
| 0x880B | PPP |
| 0x884C | MultiProtocol over ATM |
| 0x8863 | PPPoE discovery messages |
| 0x8864 | PPPoE session messages |
| 0x8884 | Frame-based ATM Transport over Ethernet |
| 0x9000 | Loopback |

# Quick Automation Profile

Ethernet Fieldbus protocols are popular in industrial automation applications. In fact, many Fieldbus protocols (e.g., EtheNet/IP and Modbus TCP/IP) can operate on an industrial Ethernet network, with the Ethernet port number defined by IANA (Internet Assigned Numbers Authority). The Industrial Secure Router provides an easy to use function called **Quick Automation Profile** that includes 45 different pre-defined profiles (Modbus TCP/IP, Ethernet/IP, etc.), allowing users to create an industrial Ethernet Fieldbus firewall policy with a single click.

For example, if the user wants to create a Modbus TCP/IP firewall policy for an internal network, the user just needs to select the **Modbus TCP/IP(TCP)** or **Modbus TCP/IP(UDP)** protocol from the **Protocol** drop-down menu on the **Firewall Policy Setting** page.




The following table shows the Quick Automation Profile for Ethernet Fieldbus Protocol and the corresponding port number

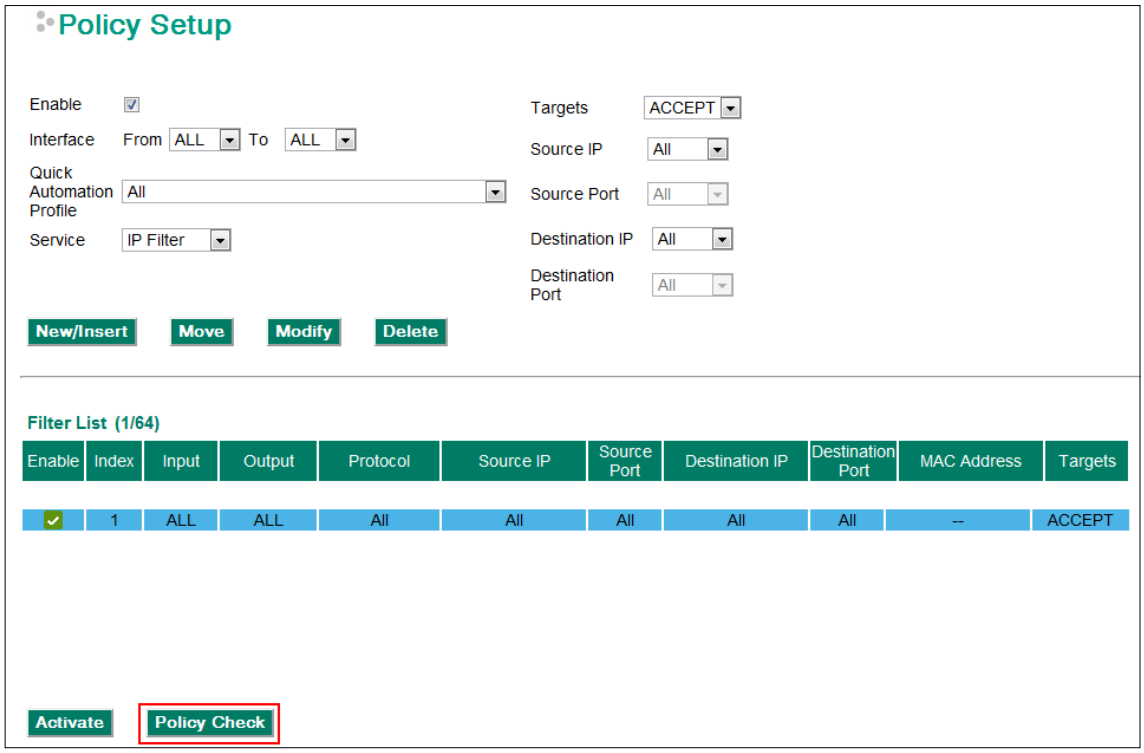
| **Ethernet Fieldbus Protocol** | **Port Number** |
|---|---|
| EtherCat port (TCP) | 34980 |
| EtherCat port (UDP) | 34980 |
| EtherNet/IP I/O (TCP) | 2222 |
| EtherNet/IP I/O (UDP) | 2222 |
| EtherNet/IP Messaging (TCP) | 44818 |
| EtherNet/IP Messaging (UDP) | 44818 |
| FF Annunciation (TCP) | 1089 |
| FF Annunciation (UDP) | 1089 |

| | |
|---|---|
| FF Fieldbus Message (TCP) | 1090 |
| FF Fieldbus Message (UDP) | 1090 |
| FF System Management (TCP) | 1091 |
| FF System Management (UDP) | 1091 |
| FF LAN Redundancy Port (TCP) | 3622 |
| FF LAN Redundancy Port (UDP) | 3622 |
| LonWorks (TCP) | 2540 |
| LonWorks (UDP) | 2540 |
| LonWorks2 (TCP) | 2541 |
| LonWorks2 (UDP) | 2541 |
| Modbus TCP/IP (TCP) | 502 |
| Modbus TCP/IP (UDP) | 502 |
| PROFInet RT Unicast (TCP) | 34962 |
| PROFInet RT Unicast (UDP) | 34962 |
| PROFInet RT Multicast (TCP) | 34963 |
| PROFInet RT Multicast (UDP) | 34963 |
| PROFInet Context Manager (TCP) | 34964 |
| PROFInet Context Manager (UDP) | 34964 |
| IEC 60870-5-104 (TCP) | 2404 |
| IEC 60870-5-104 (UDP) | 2404 |
| DNP (TCP) | 20000 |
| DNP (UDP) | 20000 |

The Quick Automation Profile also includes the commonly used Ethernet protocols listed in the following table:

| **Ethernet Protocol** | **Port Number** |
|---|---|
| IPSec NAT Traversal (UDP) | 4500 |
| IPSec NAT traversal (TCP) | 4500 |
| FTP-data (TCP) | 20 |
| FTP-data (UDP) | 20 |
| FTP-control (TCP) | 21 |
| FTP-control (UDP) | 21 |
| SSH (TCP) | 22 |
| SSH (UDP) | 22 |
| Telnet (TCP) | 23 |
| Telnet (UDP) | 23 |
| HTTP (TCP) | 80 |
| HTTP (UDP) | 80 |
| IPSec (TCP) | 1293 |
| IPSec (UDP) | 1293 |
| L2F & L2TP (TCP) | 1701 |
| L2F & L2TP (UDP) | 1701 |
| PPTP (TCP) | 1723 |
| PPTP (UDP) | 1723 |
| Radius authentication (TCP) | 1812 |
| Radius authentication (UDP) | 1812 |
| RADIUS accounting (TCP) | 1813 |
| RADIUS accounting (UDP) | 1813 |

# PolicyCheck




The Industrial Secure Router supports a **PolicyCheck** function for maintaining the firewall policy list. The **PolicyCheck** function detects firewall policies that may be configured incorrectly.

**PolicyCheck** provides an auto detection function for detecting common configuration errors in the Firewall policy (e.g., **Mask**, **Include**, and **Cross conflict)**. When adding a new firewall policy, the user just needs to click the PolicyCheck button to check each policy; warning messages will be generated that can be used for further analysis. If the user decides to ignore a warning message, the Industrial Secure Router firewall will run on the configuration provided by the user.

The three most common types of configuration errors are related to **Mask**, **Include**, and **Cross Conflict**.

## Mask: Policy [X] is masked by Policy [Y]

The Source/Destination IP range or Source/Destination port number of policy [X] is smaller or equal to policy [Y] but the action target (Accept/Drop) is different.

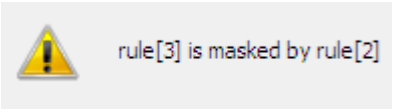
For example, two firewall policies are shown below:

| Index | Input | Output | Protocol | Source IP | Destination IP | Target |
|---|---|---|---|---|---|---|
| 1 | WAN1 | LAN | All | 10.10.10.10 | 192.168.127.10 | ACCEPT |
| 2 | WAN2 | LAN | All | 20.20.20.10<br>to 20.20.20.30 | 192.168.127.20 | ACCEPT |

Suppose the user next adds a new policy with the following configuration:

| Index | Input | Output | Protocol | Source IP | Destination IP | Target |
|---|---|---|---|---|---|---|
| 3 | WAN2 | LAN | All | 20.20.20.20 | 192.168.127.20 | DROP |

After clicking the **PolicyCheck** button, the Industrial Secure Router will issue a message informing the user that policy [3] is **masked** by policy [2] because the IP range of policy [3] is smaller than the IP range of policy [2], and the Target action is different.



## Include: Policy [X] is included in Policy [Y]

The Source/Destination IP range or Source/Destination port number of policy [X] is less than or equal to policy [Y], and the action target (Accept/Drop) is the same. In this case policy [X] will increase the loading of the Industrial Secure Router and lower its performance.

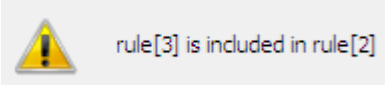
For example, two firewall policies are shown in the following table:

| Index | Input | Output | Protocol | Source IP | Destination IP | Target |
|---|---|---|---|---|---|---|
| 1 | WAN1 | LAN | All | 10.10.10.10 | 192.168.127.10 | ACCEPT |
| 2 | WAN2 | LAN | All | 20.20.20.10<br>to 20.20.20.30 | 192.168.127.20 | ACCEPT |

Suppose the user next adds a new policy with the following configuration:

| Index | Input | Output | Protocol | Source IP | Destination IP | Target |
|---|---|---|---|---|---|---|
| 3 | WAN2 | LAN | All | 20.20.20.20 | 192.168.127.20 | ACCEPT |

After clicking the **PolicyCheck** button, the Industrial Secure Router will issue a message informing the user that policy [3] is **included** in policy [2] because the IP range of policy [3] is smaller than the IP range of policy [2], and the Target action is the same.




## Cross Conflict: Policy [X] cross conflicts with Policy [Y]

Two firewall policy configurations, such as Source IP, Destination IP, Source port, and Destination port, in policy [X] and policy [Y] are masked, and the action target (Accept/Drop) is different.

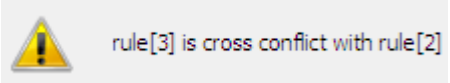
For example, two firewall policies are shown in the following table:

| Index | Input | Output | Protocol | Source IP | Destination IP | Target |
|---|---|---|---|---|---|---|
| 1 | WAN1 | LAN | All | 10.10.10.10 | 192.168.127.10 | ACCEPT |
| 2 | WAN2 | LAN | All | 20.20.20.20<br>to 20.20.20.30 | 192.168.127.25 | ACCEPT |

Suppose the user next adds a new policy with the following configuration:

| Index | Input | Output | Protocol | Source IP | Destination IP | Target |
|---|---|---|---|---|---|---|
| 3 | WAN2 | LAN | All | 20.20.20.25 | 192.168.127.20<br>to 192.168.127.30 | DROP |

The source IP range in policy 3 is smaller than policy 2, but the destination IP of policy 2 is smaller than policy 3, and the target actions (Accept/Drop) of these two policies are different. If the user clicks the **PolicyCheck** button, the Industrial Secure Router will issue a message informing the user that policy [3] is in **Cross Conflict** with policy [2].



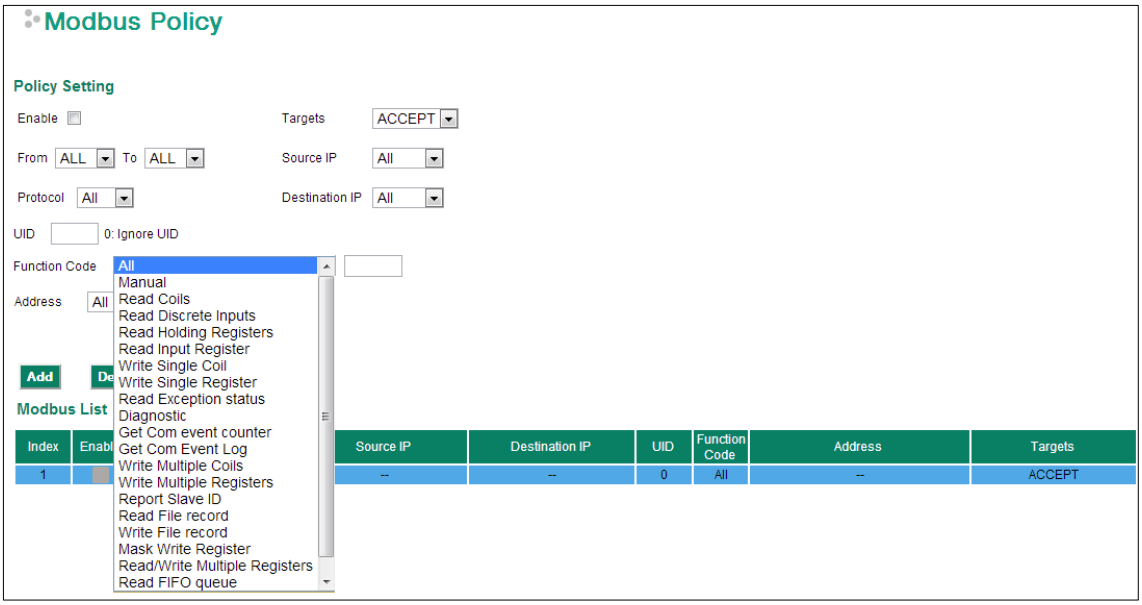
# Modbus TCP Policy Concept

Modbus TCP is a Modbus protocol used for communications over TCP/IP networks, connecting over port 502 by default. Some have experimented with using Modbus over UDP on IP networks, which removes the overheads required for TCP. The following table shows the Modbus TCP frame format:

| Modbus TCP Frame Format | | |
|---|---|---|
| **Description** | **Length** | **Function** |
| Transaction Identifier | 2 bytes | Synchronization between messages of server & client |
| Protocol Identifier | 2 bytes | The value is 0 for Modbus TCP protocol |
| Length Field | 2 bytes | Number of remaining following bytes in this frame |
| Unit Identifier | 1 byte | Slave Address (255 is used for device broadcast information) |
| Function code | 1 byte | Define message type |
| Data bytes | n bytes | Data block with additional information |

## Modbus Policy Setup

The Industrial Secure Router provides Modbus policy inspection of Modbus TCP packets, which allows users to control Modbus TCP traffic based on the following parameters:




***Add a Modbus TCP Filtering Rule***

Check the "Enable" checkbox and input the correspondent Modbus TCP parameters in the page, and then click "Add" to add it into the Modbus Filtering Table. Finally, click "Activate" to activate the configuration.

***Delete a Modbus TCP Filtering Rule***

Select the item in the Modbus Filtering Table, then, click "Delete" to delete the item.

***Modify a Modbus TCP Filtering Rule***

Select the item in the Modbus Filtering Table. Modify the attributes and click "Modify" to change the configuration.

***Activate Modbus TCP Filtering Table***

After adding/deleting/modifying any Modbus TCP Filtering Rules, make sure to click "Activate" to activate the item.

***Enable/Disable Modbus Policy***

| Setting | Description | Factory Default |
|---|---|---|
| Enable or Disable | Enable or disable the selected Modbus policy | Enabled |

***Interface From/To***

| Setting | Description | Factory Default |
|---|---|---|
| All (WAN/LAN) | Select the **From** Interface and **To** interface | From All to All |
| WAN | | |
| LAN | | |

***Protocol***

| Setting | Description | Factory Default |
|---|---|---|
| All (TCP/UDP) | This Modbus Policy will check the UDP packet, TCP packet or both. | All |
| TCP | | |
| UDP | | |

***UID***

| Setting | Description | Factory Default |
|---|---|---|
| 1 to 255 | Unit Identifier, 0 indicate this Modbus policy will check all UIDs in the packet. | 0 |

***Function Code***

| Setting | Description | Factory Default |
|---|---|---|
| Refer to the "Common function codes" section on page 3-52. | Select the function code parameters in this Modbus policy. When the function code is set to "Manual" you can set up the function code manually. | All |

***Address***

| Setting | Description | Factory Default |
|---|---|---|
| All (Address Index) | This Modbus policy will check all Data Address Index in the packet. | All |
| Single (Address Index) | This Modbus policy will check single Data Address Index in the packet. | |
| Range (Address Index) | This Modbus policy will check multiple Data Address Indexes in the packet. | |

***Target***

| Setting | Description | Factory Default |
|---|---|---|
| Accept | The packet will penetrate the firewall when it matches this Modbus policy. | Accept |
| Drop | The packet will not penetrate the firewall when it matches this Modbus policy. | |

***Source IP***

| Setting | Description | Factory Default |
|---|---|---|
| All (IP Address) | This Modbus policy will check all Source IP addresses in the packet. | All |
| Single (IP Address) | This Modbus policy will check single Source IP addresses in the packet. | |
| Range (IP Address) | This Modbus policy will check multiple Source IP addresses in the packet. | |

***Destination IP***

| Setting | Description | Factory Default |
|---|---|---|
| All (IP Address) | This Modbus policy will check all Destination IP addresses in the packet. | All |
| Single (IP Address) | This Modbus policy will check single Destination IP addresses in the packet. | |
| Range (IP Address) | This Modbus policy will check multiple Destination IP addresses in the packet. | |

Unit identifier (UID) is used with Modbus/TCP devices that are composites of several Modbus devices. It may be used to communicate via devices such as bridges and gateways which use a single IP address to support multiple independent end units.

Function code defines the message type and the type of action required by the slave. The parameter contains one byte of information. Valid function codes are in the range 1 to 255. Not all Modbus devices recognize the same set of function codes. The most common codes are supported for quick settings, and user-defined function codes are also supported.

Most function code addresses a single address or a range of addresses. The Industrial Secure Router provides code for deep data inspection.

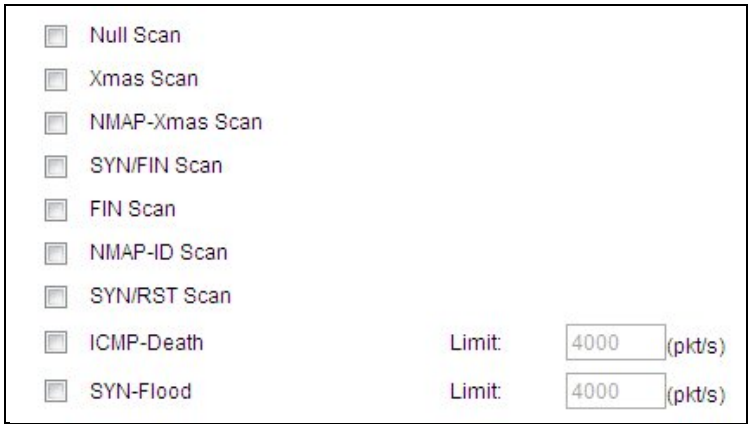
***Common function codes***

The following table shows the various reading, writing, and other operations.

| | | | Function Name | Function Code |
|---|---|---|---|---|
| Data Access | Bit Access | Physical Discrete Inputs | Read Discrete Inputs | 2 |
| | | Internal Bits or Physical Coils | Read Coils | 1 |
| | | | Write Single Coil | 5 |
| | | | Write Multiple Coils | 15 |
| | 16-bit Access | Physical Input Registers | Read Input Register | 4 |
| | | Internal Registers or Physical Output Registers | Read Holding Registers | 3 |
| | | | Write Single Register | 6 |
| | | | Write Multiple Registers | 16 |
| | | | Read/Write Multiple Registers | 23 |
| | | | Mask Write Register | 22 |
| | | | Read FIFO Queue | 24 |
| | File Record Access | | Read File Record | 20 |
| | | | Write File Record | 21 |
| Diagnostics | | | Read Exception Status | 7 |
| | | | Diagnostic | 8 |
| | | | Get Com Event Counter | 11 |
| | | | Get Com Event Log | 12 |
| | | | Report Slave ID | 17 |
| | | | Read Device Identification | 43 |

# Denial of Service (DoS) function

The Industrial Secure Router provides 9 different DoS functions for detecting or defining abnormal packet format or traffic flow. The Industrial Secure Router will drop the packets when it detects an abnormal packet format. The Industrial Secure Router will also monitor some traffic flow parameters and activate the defense process when abnormal traffic conditions are detected.




***Null Scan***

| Setting | Description | Factory Default |
|---|---|---|
| Enable or Disable | Enable or disable the Null Scan | None |

***Xmas Scan***

| Setting | Description | Factory Default |
|---|---|---|
| Enable or Disable | Enable or disable the Xmas Scan | None |

***NMAP-Xmas Scan***

| Setting | Description | Factory Default |
|---|---|---|
| Enable or Disable | Enable or disable the NMAP-Xmas | None |

***SYN/FIN Scan***

| Setting | Description | Factory Default |
|---|---|---|
| Enable or Disable | Enable or disable the SYN/FIN Scan | None |

***FIN Scan***

| Setting | Description | Factory Default |
|---|---|---|
| Enable or Disable | Enable or disable the FIN Scan | None |

***NMAP-ID Scan***

| Setting | Description | Factory Default |
|---|---|---|
| Enable or Disable | Enable or disable the NMAP-ID Scan | None |

***SYN/RST Scan***

| Setting | Description | Factory Default |
|---|---|---|
| Enable or Disable | Enable or disable the SYN/RST Scan | None |

***ICMP-Death***

| Setting | Description | Factory Default |
|---|---|---|
| Enable or Disable | Enable or disable the ICMP-Death defense | None |
| Packet/Second | The limit value to activate ICMP-Death defense | None |

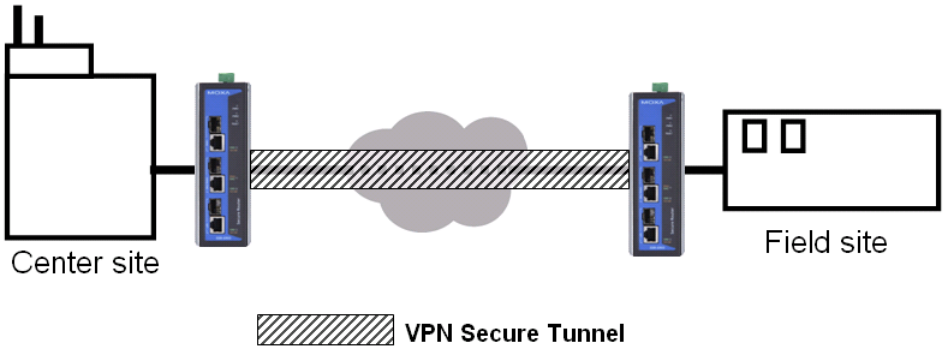
***SYN-Flood***

| Setting | Description | Factory Default |
|---|---|---|
| Enable or Disable | Enable or disable the Null Scan function | None |
| Packet/Second | The limit value to activate SYN-Flood defense | None |

# VPN (Virtual Private Network, EDR-G902/G903 and EDR-810-VPN only)

## Overview

In this section we describe how to use the Industrial Secure Router to build a secure Remote Automation network with the VPN (Virtual Private Network) feature. A VPN provides a highly cost effective solution of establishing secure tunnels, so that data can be exchanged in a secure manner.




There are two common applications for secure remote communication in an industrial automation network:

**IPSec (Internet Protocol Security) VPN for LAN to LAN Security:** Data communication only in a pre-defined IP range between two different LANs.

**L2TP (Layer 2 Tunnel Protocol) VPN for Remote roaming User:** Secure data communication for remote roaming users with dynamic IP. L2TP is a popular choice for remote roaming users for VPN applications because the L2TP VPN protocol is already built in to the Microsoft Windows operating system.

IPSec uses IKE (Internet Key Exchange) protocol for Authentication, Key exchange and provides a way for the VPN gateway data to be protected by different encryption methods.

There are 2 phases for IKE for negotiating the IPSec connections between 2 VPN gateways:

**Key Exchange (IPSec Phase 1):** The 2 VPN gateways will negotiate how IKE should be protected. Phase 1 will also authenticate the two VPN gateways by the matched Pre-Shared Key or X.509 Certificate.

**Data Exchange (IPSec Phase 2):** In Phase 2, the VPN gateways negotiate to determine additional IPSec connection details, which include the data encryption algorithm.

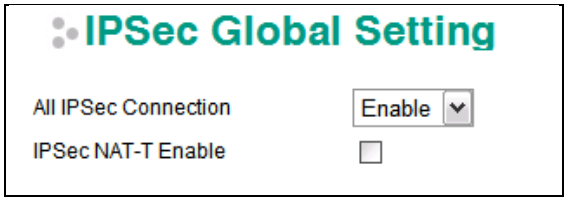
## IPSec Configuration

IPSec configuration includes 5 parts:

- **Global Setting:** Enable / Disable all IPSec Tunnels and NAT-Traversal function
- **Tunnel Setting:** Set up the VPN Connection type and VPN network plan
- **Key Exchange:** Authentication for 2 VPN gateways
- **Data Exchange:** Data encryption between VPN gateways
- **Dead Peer Detection:** The mechanism for VPN Tunnel maintenance.

## Global Configuration

The Industrial Secure Router provides 2 Global Settings for VPN applications.




### All IPSec Connection

Users can Enable or Disable all VPN services with this configuration.

**NOTE** The factory default setting is Disable, so when the user wants to use VPN function, make sure the setting is enabled.

### IPSec NAT-T

If there is an external NAT device between VPN tunnels, the user must enable the NAT-T (NAT-Traversal) function.

## IPSec Quick Setting

The Industrial Secure Router's **Quick Setting** mode can be used to easily set up a site-to-site VPN tunnel for two Industrial Secure Router units.

When choosing the Quick setting mode, the user just needs to configure the following:

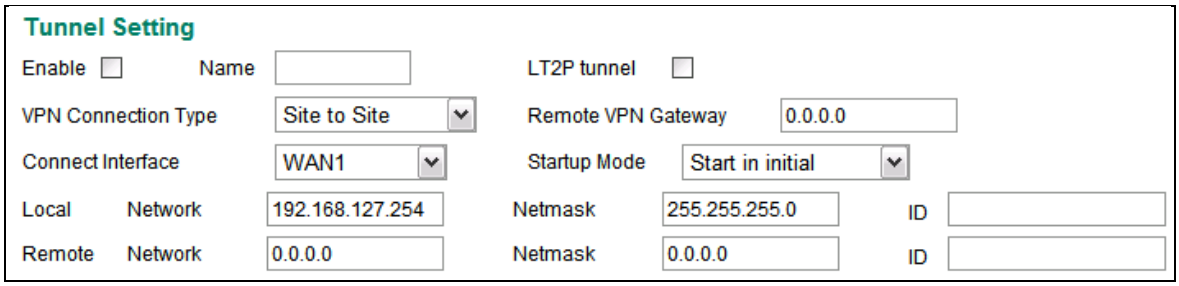
- Tunnel Setting
- Security Setting
  - Encryption Strength: Simple (AES-128), Standard (AES-192), Strong (AES-256)
  - Password of Pre-Shared Key

**NOTE** The Encryption strength and Pre-Shared key should be configured identically for both Industrial Secure Router units.

## IPSec Advanced Setting

Click **Advanced Setting** to configure detailed VPN settings.

## Tunnel Setting




***Enable or Disable VPN Tunnel***

| Setting | Description | Factory Default |
|---|---|---|
| Enable or Disable | Enable or Disable this VPN Tunnel | Disable |

***Name of VPN Tunnel***

| Setting | Description | Factory Default |
|---|---|---|
| Max. of 16 characters | User defined name of this VPN Tunnel. | None |

**NOTE** The first character cannot be a number.

***L2TP over IPSec Enable or Disable***

| Setting | Description | Factory Default |
|---|---|---|
| Enable or Disable | Enable or Disable IPSec tunnel over L2TP protocol function | None |

***VPN Connection Type***

| Setting | Description | Factory Default |
|---|---|---|
| Site to Site | VPN tunnel for Local and Remote subnets are fixed | Site to Site |
| Site to Site (Any) | VPN tunnel for Remote subnet area is dynamic and Local subnet is fixed | |

***Remote VPN Gateway***

| Setting | Description | Factory Default |
|---|---|---|
| IP Address | Remote VPN Gateway's IP Address | None |

***Connection Interface***

| Setting | Description | Factory Default |
|---|---|---|
| WAN1<br>WAN2<br>Default Route | The interface of the VPN Tunnel<br>If the user enables the WAN backup function, WAN1 would be the primary default route and WAN2 would be the backup route. | WAN1 |

***Startup Mode***

| Setting | Description | Factory Default |
|---|---|---|
| Start in Initial | This VPN tunnel will actively initiate the connection with the Remote VPN Gateway. | Start in Initial |
| Wait for Connecting | This VPN tunnel will wait remote VPN gateway to initiate the connection | |

**NOTE** The maximum number of **Starts** in the initial VPN tunnel is 30. The maximum number of **Waits** for connecting to a VPN tunnel is 100.

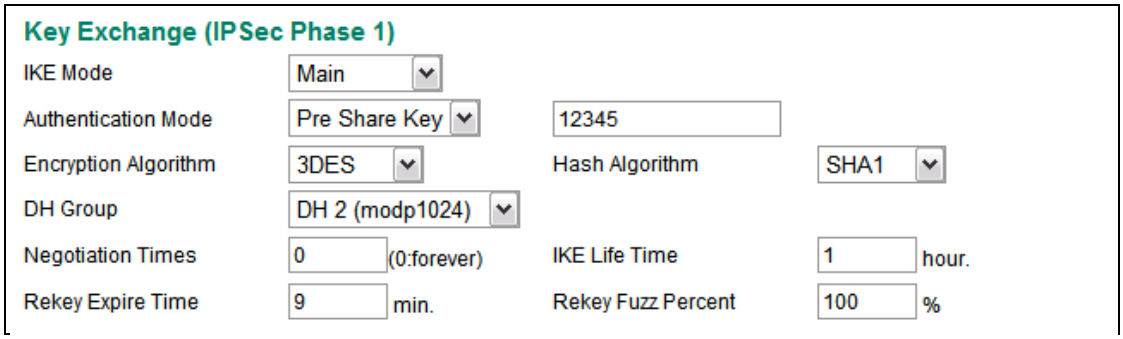
***Local Network / Netmask / ID***

| Setting | Description | Factory Default |
|---|---|---|
| IP Address | IP address of local VPN network | IP address of LAN interface |
| Subnet Mask | Subnet Mask of local VPN network | Netmask of LAN interface |
| ID | ID for indentifying the VPN tunnel connection.<br>The Local ID must be equal to the Remote ID of the VPN Gateway. Otherwise, the VPN tunnel cannot be established successfully | None |

***Remote Network / Netmask / ID***

| Setting | Description | Factory Default |
|---|---|---|
| IP Address | IP address of Remote VPN network | 0.0.0.0 |
| Subnet Mask | Subnet Mask of local VPN network | 0.0.0.0 |
| ID | ID for indentifying the VPN tunnel connection.<br>The Local ID must be equal to the Remote ID of the VPN Gateway. Otherwise, the VPN tunnel cannot be established. | None |

## Key Exchange (IPSec phase I)



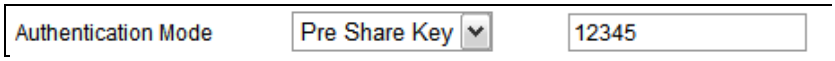

***IKE Mode***

| Setting | Description | Factory Default |
|---|---|---|
| Main | In "Main" IKE Mode, both the Remote and Local VPN gateway will negotiate which Encryption/Hash algorithm and DH groups can be used in this VPN tunnel; both VPN gateways must use the same algorithm to communicate. | MAIN |
| Aggressive | In "Aggressive" Mode, the Remote and Local VPN gateway will not negotiate the algorithm; it will use the user's configuration only. | |

***Authentication Mode***

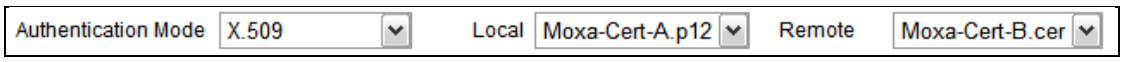
| Setting | Description | Factory Default |
|---|---|---|
| Pre-Shared Key | The authentication mode of IPSec VPN | Pre-Shared Key |
| X.509 | | |

In **Pre-Shared Key Mode**, the user needs to key-in the same Pre-Shared Key in the IPSec setting between the Local and Remote secure router.




In **X.509 Mode**, the user needs to upload the Local and Remote certifications first, and then select the certifications from the drop-down list.

See the **X.509 Certification** section in this chapter for details.




***Encryption Algorithm***

| Setting | Description | Factory Default |
|---|---|---|
| DES<br>3DES<br>AES-128<br>AES-192<br>AES-256 | Encryption Algorithm in key exchange | 3DES |

***Hash Algorithm***

| Setting | Description | Factory Default |
|---|---|---|
| Any<br>MD5<br>SHA1<br>SHA256 | Hash Algorithm in key exchange | SHA1 |

***DH Group***

| Setting | Description | Factory Default |
|---|---|---|
| DH1(modp 768)<br>DH2(modp 1024)<br>DH5(modp 1536)<br>DH14(modp 2048) | Diffie-Hellman groups<br>(the Key Exchange group between the Remote and VPN Gateways) | DH2(modp 1024) |

***Negotiation Time***

| Setting | Description | Factory Default |
|---|---|---|
| Negotiation time | The number of allowed reconnect times when startup mode is initiated. If the number is **0**, this tunnel will always try connecting to the remote gateway when the VPN tunnel is not created successfully. | 0 |

***IKE Lifetime***

| Setting | Description | Factory Default |
|---|---|---|
| IKE lifetime (hours) | Lifetime for IKE SA | 1 (hr) |

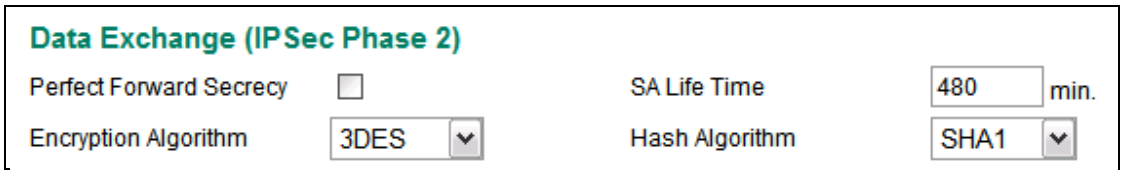
***Rekey Expire Time***

| Setting | Description | Factory Default |
|---|---|---|
| Rekey expire time (minutes) | Start to Rekey before IKE lifetime expired | 9 (min) |

***Rekey Fuzz Percent***

| Setting | Description | Factory Default |
|---|---|---|
| 0-100 (%) | The rekey expire time will change randomly to enhance the security.<br>Rekey fuzz percent is the maximum random change margin of the Rekey expire time.<br>100% means the rekey expire time will not change randomly. | 100 (%) |

## Data Exchange (IPSec phase II)




***Perfect Forward Secrecy***

| Setting | Description | Factory Default |
|---|---|---|
| Enable or Disable | Uses different security key for different IPSec phases to enhance security | Disable |

***SA Lifetime***

| Setting | Description | Factory Default |
|---|---|---|
| SA lifetime (minutes) | Lifetime for SA in Phase 2 | 480 (min) |

***Encryption Algorithm***

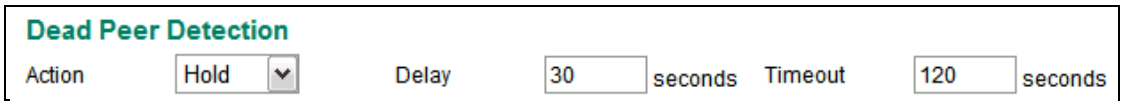
| Setting | Description | Factory Default |
|---|---|---|
| DES<br>3DES<br>AES-128<br>AES-192<br>AES-256 | Encryption Algorithm in data exchange | 3DES |

***Hash Algorithm***

| Setting | Description | Factory Default |
|---|---|---|
| Any<br>MD5<br>SHA1<br>SHA256 | Hash Algorithm in data exchange | SHA1 |

## Dead Peer Detection

Dead Peer Detection is a mechanism to detect whether or not the connection between a local secure router and a remote IPSec tunnel has been lost.




***Action***

Action when a dead peer is detected.

| Setting | Description | Factory Default |
|---|---|---|
| Hold | Hold this VPN tunnel | Hold |
| Restart | Reconnect this VPN tunnel | |
| Clear | Clear this VPN tunnel | |
| Disable | Disable Dead Peer Detection | |

***Delay***

| Setting | Description | Factory Default |
|---|---|---|
| Delay time (seconds) | The period of dead peer detection messages | 30 (sec) |

***Timeout***

| Setting | Description | Factory Default |
|---|---|---|
| Timeout (seconds) | Timeout to check if the connection is alive or not | 120 (sec) |

## IPSec Status

The user can check the VPN tunnel status in the **IPSec Connection List**.

This list shows the Name of the IPSec tunnel, IP address of Local and Remote Subnet/Gateway, and the established status of the Key exchange phase and Data exchange phase.

**IPSec Connection List**

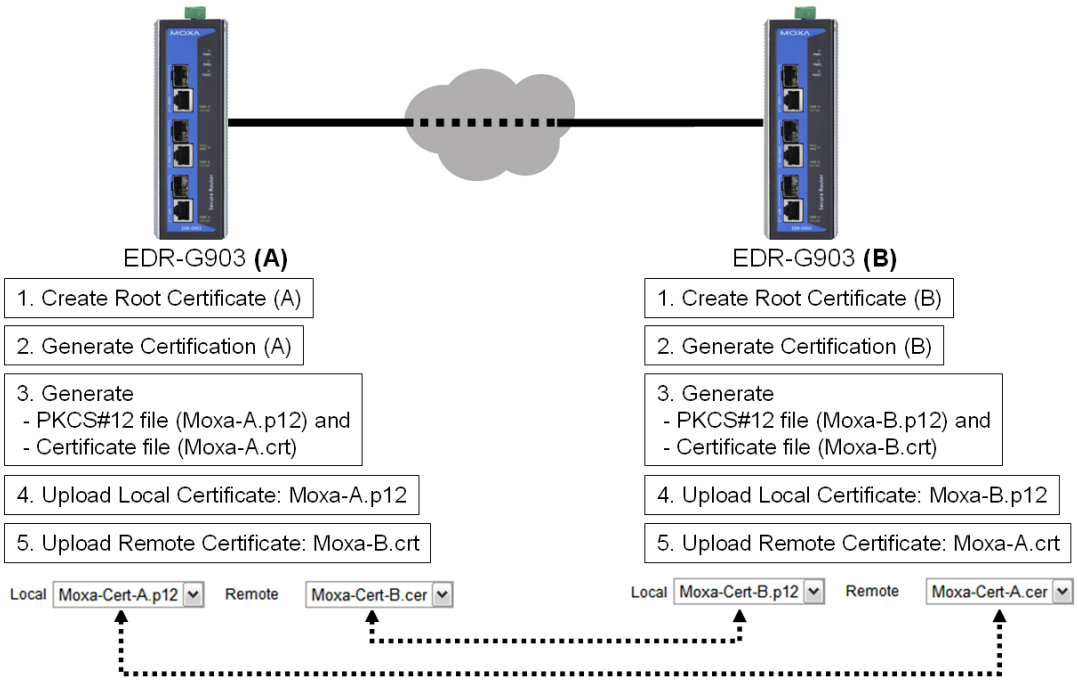
| Name | Local Subnet | Local Gateway | Remote Gateway | Remote Subnet | Key Exchange (IPSec Phase 1) | Data Exchange (IPSec Phase 2) |
|---|---|---|---|---|---|---|

# X.509 Certification

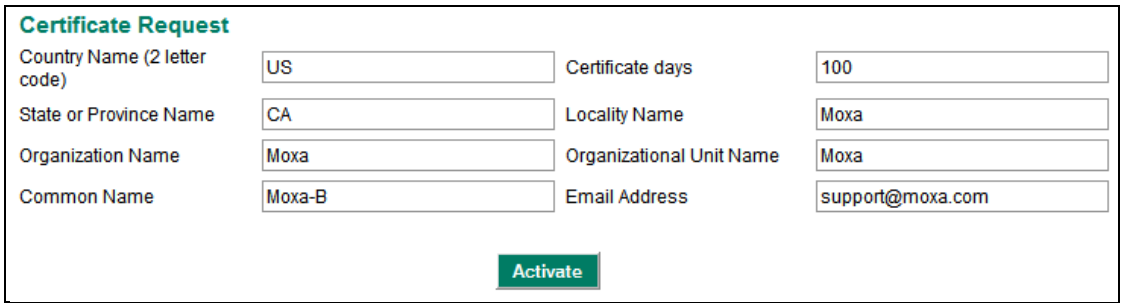
X.509 is a digital certificate method commonly used for IPSec Authentication. The Industrial Secure Router can generate a trusted Root Certification and then export/import the certificate to the remote VPN gateway.

The diagram below indicates the 5 steps you should follow to use X.509 for IPSec authentication with two VPN gateways, referred to as EDR-G903(A) and EDR-G903(B) in the diagram:

1. Root Certificate generation. Both EDR-G903(A) and EDR-G903(B) need to generate their own root certificates.
2. EDR-G903(A) and EDR-G903(B) can request new certifications based on their own Root Certificates.
3. Generate PKCS#12 local certificate with password (.p12) and Certificate file for remote VPN tunnel (.crt)
   a. EDR-G903(A)→Moxa-A.p12 and Moxa-A.crt
   b. EDR-G903(B)→Moxa-B.crt and Moxa-B.crt
4. Upload the PKCS#12 certificate to the Local Certification list
   a. Moxa-A.p12 in EDR-G903(A)
   b. Moxa-B.p12 in EDR-G903(B)
5. Send the Certificate file (.crt) to the remote VPN gateway and upload to the Remote certificate file
   a. Upload Moxa-B.crt to EDR-G903(A)
   b. Upload Moxa-A.crt to EDR-G903(B)



## Certificate Generation



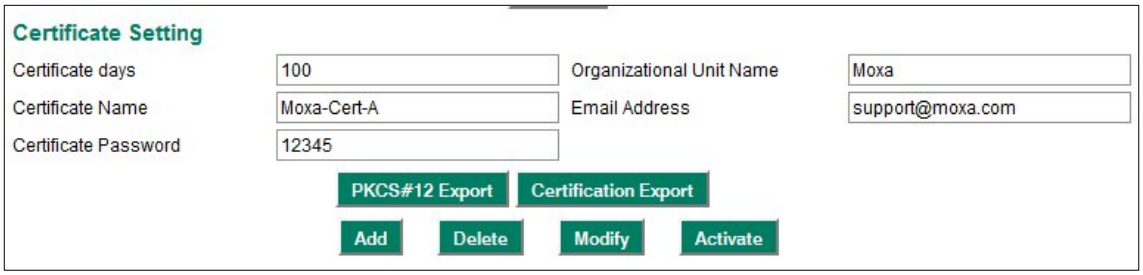

The user must fill in the following information to generate the Root certification:

- Country name (2 Letter code)
- Certificate Days
- State or Province Name
- Locality Name
- Organization Name
- Organization Unit Name
- Common Name
- Email Address

After keying in all of the information, press **Activate** to generate the Root Certification.

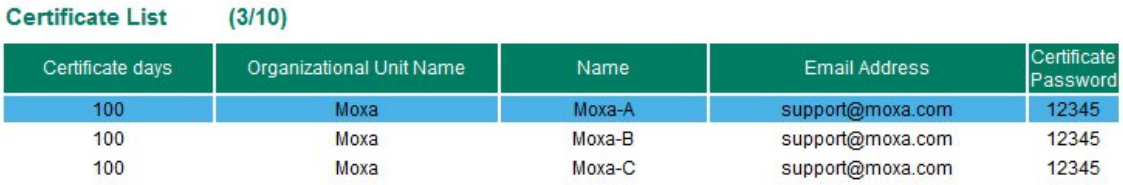
**NOTE** The default setting for Certificate Day is 0, which means that the certification will not be terminated unless modified by the user.

## Certificate Setting



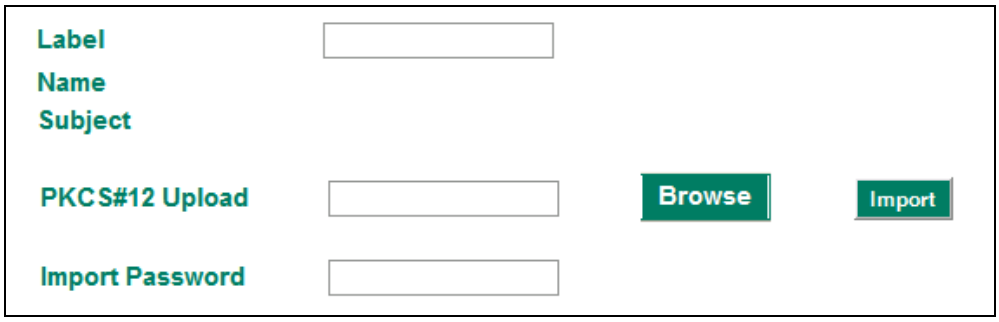

After Root Certification is activated, the user can generate different certifications for different VPN Tunnels. The user needs to fill in the following information and press **Add and Activate** to add the new certificate to the **Certificate List**.

- Certificate Days
- Organization Unit Name
- Certificate Name
- Email Address
- Certificate Password




The user can then choose certificates from the list and press the **PKCS#12 Export** button to generate a **.p12** file for a local certificate and press **Certificate Export** to generate a **.crt** file for certificates on a Remote VPN gateway.

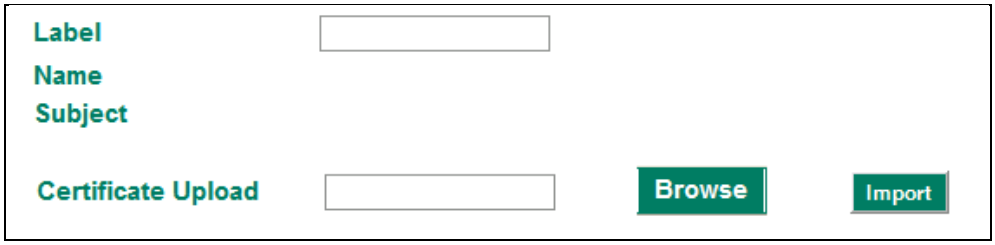
## Local Certificate Upload




Upload the .p12 local certificate on this page. The Password must be the same as the .p12 certificate file. If the password is not correct, the certificate import process will fail.

**Label**: User defined name for this local certificate
**Name/Subject**: Show the Name and subject when the certificate is imported successfully or the user selects the certificate on the list
**PKCS#12 Upload**: Use Browser to select the .p12 file and press the Import button
**Import Password**: The Password for the .p12 certificate

## Remote Certificate Upload



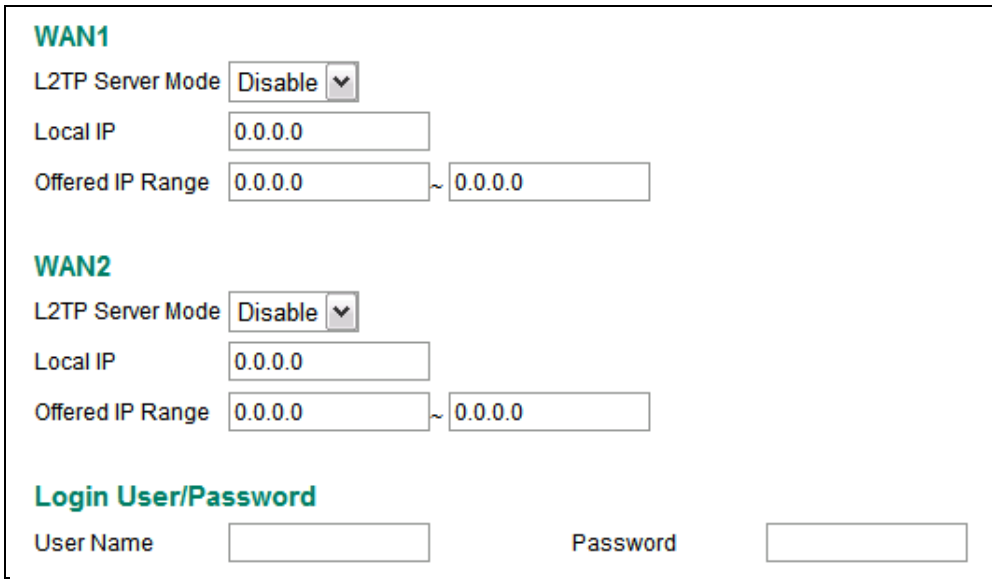

Upload the .crt Remote certificate on this page.

**Label**: User defined name for this local certificate
**Name/Subject**: Show the Name and subject when the certificate is imported successfully or the user selects a certificate from the list
**Certificate Upload**: Use the Browser to select a .p12 file and press the Import button.

# L2TP (Layer 2 Tunnel Protocol)

L2TP is a popular choice for remote roaming users for VPN applications since an L2TP client is built in to the Microsoft Windows operating system. Since L2TP does not provide an encryption function, it is usually combined with IPSec to provide data encryption.

## L2TP Configuration




***L2TP Server Mode***

| Setting | Description | Factory Default |
|---|---|---|
| Enable / Disable | Enable or Disable the L2TP function on the WAN1 or WAN 2 interface | Disable |

***Local IP***

| Setting | Description | Factory Default |
|---|---|---|
| IP Address | The IP address of the Local Subnet | 0.0.0.0 |

***Offered IP Range***

| Setting | Description | Factory Default |
|---|---|---|
| IP Address | Offered IP range is for the L2TP clients | 0.0.0.0 |

***Login User Name***

| Setting | Description | Factory Default |
|---|---|---|
| Max. to xx character. | User Name for L2TP connection | NULL |

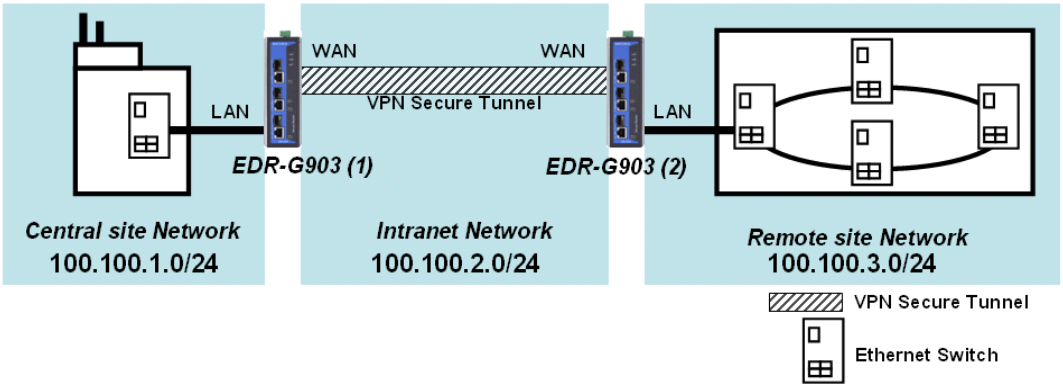
***Login Password***

| Setting | Description | Factory Default |
|---|---|---|
| Max. to xx character. | Password for L2TP connection | NULL |

# Examples for Typical VPN Applications

## Site to Site IPSec VPN tunnel with Pre-Shared Key

The following example shows how to create a secure LAN to LAN VPN tunnel between the Central site and Remote site via an Intranet network.




### VPN Plan

- All communication from the Central site network (100.100.1.0/24) to the Remote site Network (100.100.3.0/24) needs to pass through the VPN tunnel.
- Intranet Network is 100.100.2.0/24
- The configuration of the WAN/LAN interface for 2 Industrial Secure Routers is shown in the following table.

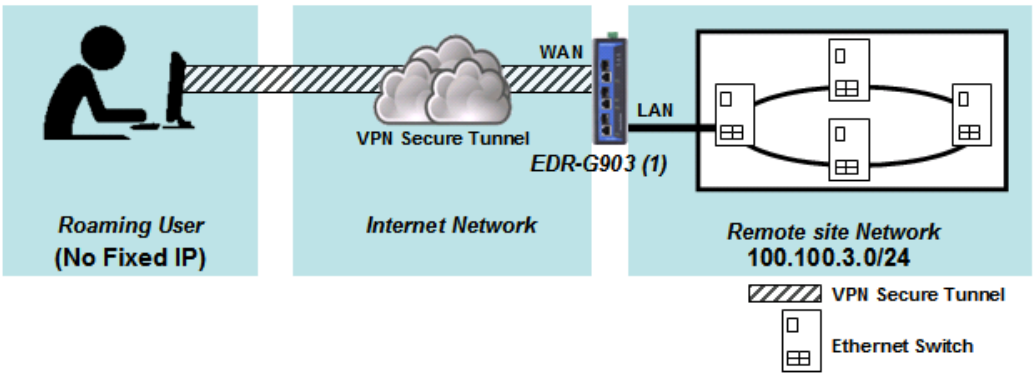
| | Configuration | Industrial Secure Router (1) | Industrial Secure Router (2) |
|---|---|---|---|
| EDR-G903 Interface Setting | WAN IP | 100.100.2.1 | 100.100.2.2 |
| | LAN IP | 100.100.1.1 | 100.100.3.1 |

Based on the requirement and VPN plan, the recommended configuration for VPN IPSec is shown in the following table

| | Configuration | Industrial Secure Router (1) | Industrial Secure Router (2) |
|---|---|---|---|
| Tunnel Setting | Connection Type | Site to Site | Site to Site |
| | Remote VPN gateway | 100.100.2.2 | 100.100.2.1 |
| | Startup mode | Wait for Connection | Start in Initial |
| | Local Network / Netmask | 100.100.1.0 / 255.255.255.0 | 100.100.3.0 / 25.255.255.0 |
| | Remote Network / Netmask | 100.100.3.0 / 25.255.255.0 | 100.100.1.0 / 255.255.255.0 |
| Key Exchange | Pre-Shared Key | 12345 | 12345 |
| Data Exchange | Encryption / Harsh | 3DES / SHA1 | 3DES / SHA1 |

## L2TP for Remote User Maintenance

The following example shows how a Roaming user uses L2TP over IPSec to connect to the remote site network.




### VPN Plan

- All communication from the Roaming user (no fixed IP) to the Remote site Network (100.100.3.0/24) needs to pass through the VPN tunnel.
- Communication goes through the Internet.
- The configuration of the WAN/LAN interface for the Industrial Secure Router is shown in the following table.

| | Configuration | Industrial Secure Router (1) |
|---|---|---|
| EDR-G903 Interface Setting | WAN IP | 100.100.2.1 |
| | LAN IP | 100.100.3.1 |

Based on the requirement and VPN plan, the recommended configuration for L2TP over IPSec is shown in the following table:

| | Configuration | Industrial Secure Router (1) |
|---|---|---|
| L2TP Server Setting | L2TP Server Mode (WAN1) | Enable |
| | Local IP (L2TP Server IP) | 100.100.4.1 |
| | Offer IP Range | 100.100.4.1 ~100.100.4.100 |
| | Login User / Password | User01 / 12345 |
| Tunnel Setting | Connection Type | Site to Site (Any) |
| | L2TP Tunnel | Enable |
| | Local Network | 100.100.3.1 / 24<br>(Same as LAN Interface) |
| | Startup mode | Wait for Connection |
| Key Exchange | Pre-Shared Key | 12345 |
| Data Exchange | Encryption Algorithm<br>Harsh Algorithm | 3DES<br>SHA1 |

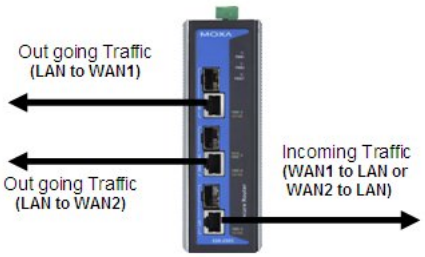
# Traffic Prioritization

The Industrial Secure Router's traffic prioritization capability provides Quality of Service (QoS) to your network by making data delivery more reliable. You can prioritize traffic on your network to ensure that high priority data is transmitted with minimum delay. Traffic can be controlled by a set of rules to obtain the required Quality of Service for your network.

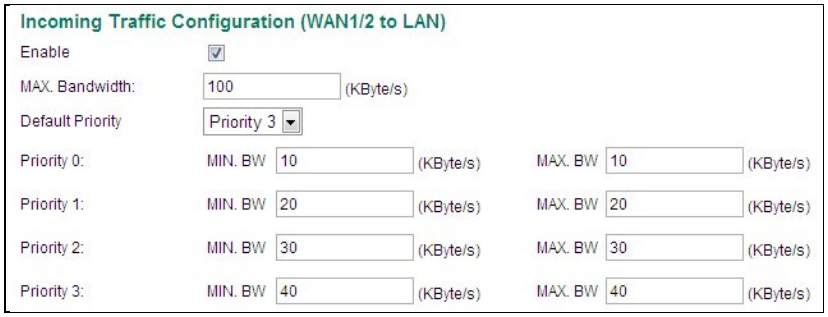
**NOTE** The maximum number of traffic prioritization policies for the Industrial Secure Router is 256.

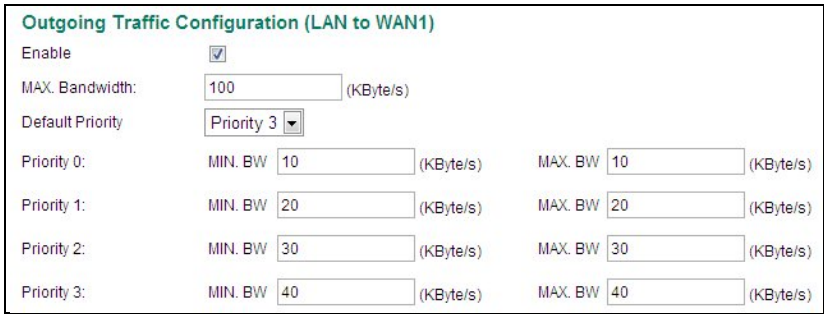
# How Traffic Prioritization Works

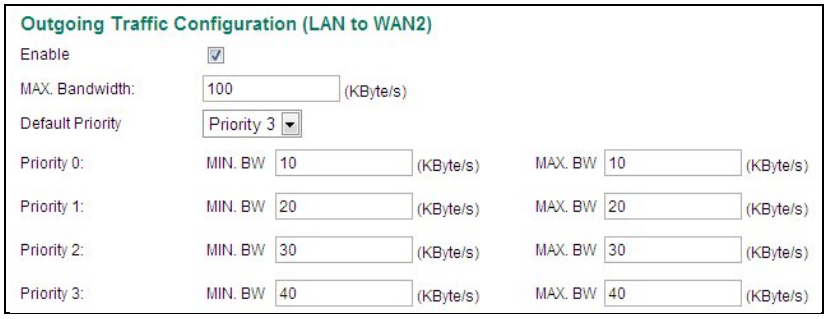
The Industrial Secure Router provides four different priorities levels (0-3, high to low) for incoming and outgoing traffic. The following figure illustrates incoming traffic, which refers to the traffic transmitted from WAN1 to LAN or WAN2 to LAN interface. Outgoing traffic refers to the traffic transmitted from LAN to WAN1 or from LAN to WAN2.




The following figures show the configuration for incoming and outgoing traffic. Users can manage the priority of incoming traffic (WAN1 to LAN and WAN2 to LAN) and outgoing traffic (LAN to WAN1 and LAN to WAN2).


Incoming Traffic Configuration (WAN1/2 to LAN)
Enable
MAX. Bandwidth: 100 (KByte/s)
Default Priority Priority 3
Priority 0: MIN. BW 10 (KByte/s) MAX. BW 10 (KByte/s)
Priority 1: MIN. BW 20 (KByte/s) MAX. BW 20 (KByte/s)
Priority 2: MIN. BW 30 (KByte/s) MAX. BW 30 (KByte/s)
Priority 3: MIN. BW 40 (KByte/s) MAX. BW 40 (KByte/s)


Outgoing Traffic Configuration (LAN to WAN1)
Enable
MAX. Bandwidth: 100 (KByte/s)
Default Priority Priority 3
Priority 0: MIN. BW 10 (KByte/s) MAX. BW 10 (KByte/s)
Priority 1: MIN. BW 20 (KByte/s) MAX. BW 20 (KByte/s)
Priority 2: MIN. BW 30 (KByte/s) MAX. BW 30 (KByte/s)
Priority 3: MIN. BW 40 (KByte/s) MAX. BW 40 (KByte/s)


Outgoing Traffic Configuration (LAN to WAN2)
Enable
MAX. Bandwidth: 100 (KByte/s)
Default Priority Priority 3
Priority 0: MIN. BW 10 (KByte/s) MAX. BW 10 (KByte/s)
Priority 1: MIN. BW 20 (KByte/s) MAX. BW 20 (KByte/s)
Priority 2: MIN. BW 30 (KByte/s) MAX. BW 30 (KByte/s)
Priority 3: MIN. BW 40 (KByte/s) MAX. BW 40 (KByte/s)

# Traffic Prioritization Configuration (EDR-G902/G903 series)

***Enable or Disable***

| Setting | Description | Factory Default |
|---|---|---|
| Enable or Disable | Enable or disable the Traffic Prioritization function | Disabled |

***Max. Bandwidth***

| Setting | Description | Factory Default |
|---|---|---|
| 1 to 1,000,000 KBytes/s | The maximum bandwidth for total incoming or outgoing traffic | 100 KBytes/s |

***Default Priority***

| Setting | Description | Factory Default |
|---|---|---|
| Priority 0/1/2/3 | A packet without matching any incoming/outgoing policy will adhere to the default priority | Priority 3 |

***Minimum Bandwidth of Priority 0/1/2/3***

| Setting | Description | Factory Default |
|---|---|---|
| 1 to 1,000,000 KBytes/s | The minimum bandwidth for Priority 0/1/2/3 | Priority 0: 10 KBytes/s<br>Priority 1: 20 KBytes/s<br>Priority 2: 30 KBytes/s<br>Priority 3: 40 KBytes/s |

***Maximum Bandwidth of Priority 0/1/2/3***

| Setting | Description | Factory Default |
|---|---|---|
| 1 to 1,000,000 KBytes/s | The maximum bandwidth for Priority 0/1/2/3 | Priority 0: 10 KBytes/s<br>Priority 1: 20 KBytes/s<br>Priority 2: 30 KBytes/s<br>Priority 3: 40 KBytes/s |

## Outgoing/Incoming Policy Setup

After configuring the minimum/maximum bandwidth for each priority, users can set up the incoming or outgoing policies for Ethernet traffic, providing the setup meets all of the following conditions:

***Enable or Disable***

| Setting | Description | Factory Default |
|---|---|---|
| Enable or Disable | Enable or disable this Incoming or Outgoing Policy | Disabled |

***Packet To / From***

| Setting | Description | Factory Default |
|---|---|---|
| All (WAN1 or WAN2) | Select the direction of Ethernet traffic for this policy<br>To: For outgoing policy<br>From: For incoming policy | All |
| WAN1 | | |
| WAN2 | | |

***Protocol***

| Setting | Description | Factory Default |
|---|---|---|
| All (TCP/UDP/ICMP) | Select the Protocol for in this Policy | All |
| TCP | | |
| UDP | | |
| ICMP | | |

***Service***

| Setting | Description | Factory Default |
|---|---|---|
| By IP | Select the service type (IP address or MAC address) for this policy | By IP |
| By MAC | | |

***Priority***

| Setting | Description | Factory Default |
|---|---|---|
| Priority 0/1/2/3 | Select the priority for this policy | Priority 0 |

***Source IP***

| Setting | Description | Factory Default |
|---|---|---|
| All (IP Address) | Select the Source IP address for this policy | All |
| Single (IP Address) | | |
| Range (IP Address) | | |

***Source Port***

| Setting | Description | Factory Default |
|---|---|---|
| All (Port number) | Select the Source port number for this policy | All |
| Single (Port number) | | |
| Range (Port number) | | |

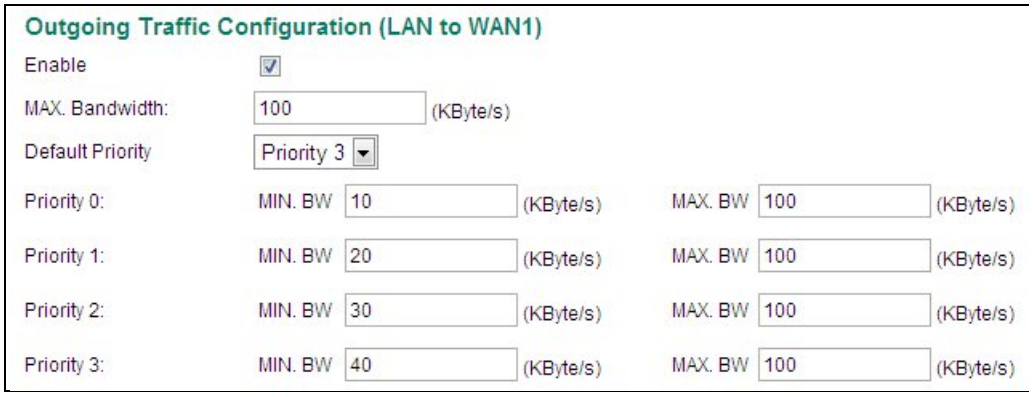
***Destination IP***

| Setting | Description | Factory Default |
|---|---|---|
| All (IP Address) | Select the Destination IP address for this policy | All |
| Single (IP Address) | | |
| Range (IP Address) | | |

***Destination Port***

| Setting | Description | Factory Default |
|---|---|---|
| All (Port number) | Select the Destination port number for this policy | All |
| Single (Port number) | | |
| Range (Port number) | | |

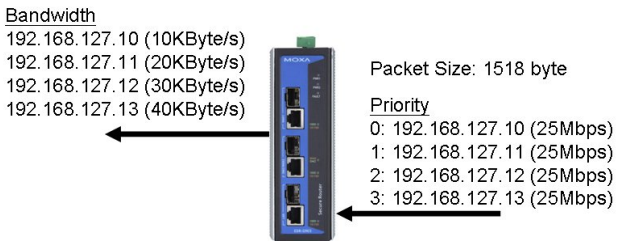
The following table shows the management of outgoing traffic. The maximum bandwidth from LAN to WAN is 100 Kbytes. 10 Kbyte is reserved for traffic that matches the parameters of Priority 0. 20 Kbytes is reserved for traffic that matches the parameters of priority 1 and so forth.


Outgoing Traffic Configuration (LAN to WAN1)
Enable
MAX. Bandwidth: 100 (KByte/s)
Default Priority Priority 3
Priority 0: MIN. BW 10 (KByte/s) MAX. BW 100 (KByte/s)
Priority 1: MIN. BW 20 (KByte/s) MAX. BW 100 (KByte/s)
Priority 2: MIN. BW 30 (KByte/s) MAX. BW 100 (KByte/s)
Priority 3: MIN. BW 40 (KByte/s) MAX. BW 100 (KByte/s)

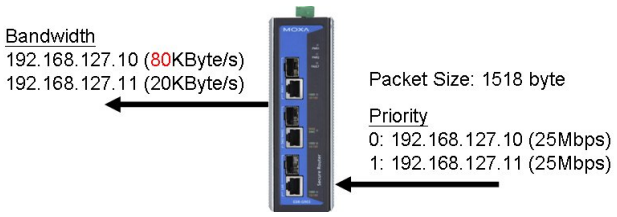
Set up the outgoing policies as below:

| Index | Output | Protocol | Source IP | Source Port | Destination IP | Destination Port | MAC Address | Targets |
|---|---|---|---|---|---|---|---|---|
| 1 | WAN1 | All | 192.168.127.10 | All | All | All | -- | Priority 0 |
| 2 | WAN1 | All | 192.168.127.11 | All | All | All | -- | Priority 1 |
| 3 | WAN1 | All | 192.168.127.12 | All | All | All | -- | Priority 2 |
| 4 | WAN1 | All | 192.168.127.13 | All | All | All | -- | Priority 3 |

The Industrial Secure Router will manage the bandwidth for outgoing packets. Based on the four outgoing policies below, when the source IP of the Ethernet traffic matches the outgoing policies, the maximum bandwidth for a packet sent from these source IP addresses will be reserved by its target priority.




If there are only two kinds of traffic packets, priority 0 and priority 1, then transmission will proceed from LAN to WAN1, and the Industrial Secure Router will reserve the minimum bandwidth (10 KBytes/s and 20 Kbyte/s) based on these two different IP addresses. In this case, there are still 100 KBytes/s - 10 KBytes/s - 20 KBytes/s = 70 KBytes/s that do not belong to any priority. So, the Industrial Secure Router will increase the bandwidth from highest priority (0) to lowest priority (3). The Industrial Secure Router will add this 70 KBytes/s bandwidth to priority 0 because the maximum bandwidth of priority 0 is 100 KBytes/s. The figure to the above right shows the bandwidth arrangement of the Industrial Secure Router based on this configuration.



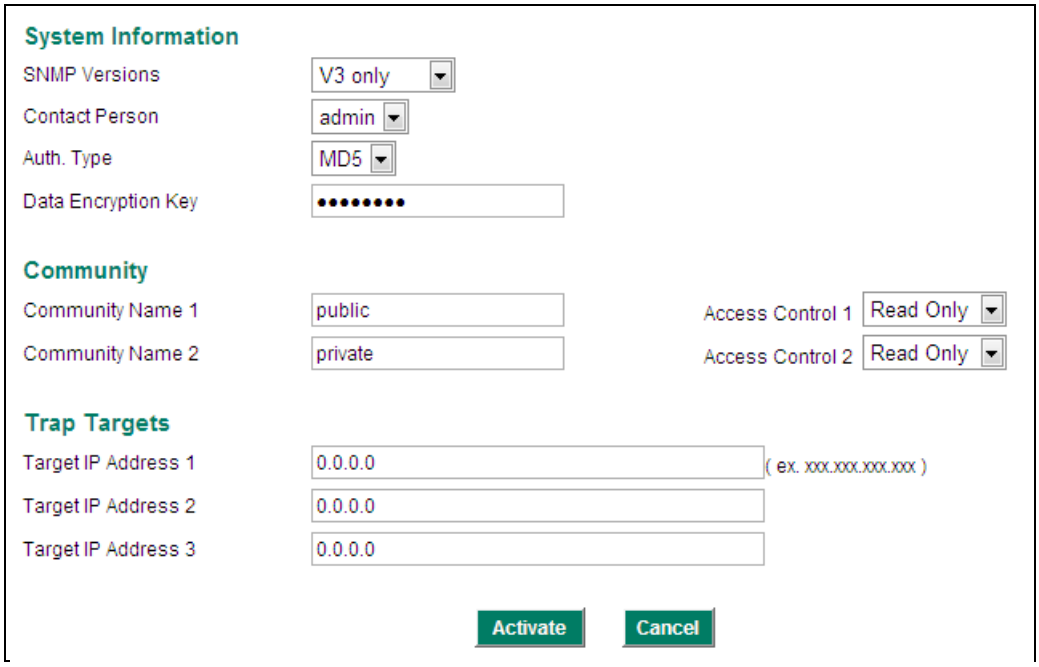

# Configuring SNMP

The Industrial Secure Router supports SNMP V1/V2c/V3. SNMP V1 and SNMP V2c use a community string match for authentication, which means that SNMP servers access all objects with read-only permissions using the community string public (default value). SNMP V3, which requires that the user selects an authentication level of MD5 or SHA, is the most secure protocol. You can also enable data encryption to enhance data security. SNMP security modes and security levels supported by the Industrial Secure Router are shown in the following table. Select the security mode and level that will be used to communicate between the SNMP agent and manager.

| Protocol Version | UI Setting | Authentication Type | Data Encryption | Method |
|---|---|---|---|---|
| SNMP V1, V2c | V1, V2c Read Community | Community string | No | Uses a community string match for authentication |
| SNMP V3 | MD5 or SHA | Authentication based on MD5 or SHA | No | Provides authentication based on HMAC-MD5, or HMAC-SHA algorithms. 8-character passwords are the minimum requirement for authentication. |
| | MD5 or SHA | Authentication based on MD5 or SHA | Data encryption key | Provides authentication based onHMAC-MD5 or HMAC-SHA algorithms, and data encryption key. 8-character passwords and a data encryption key are the minimum requirements for authentication and encryption. |

These parameters are configured on the SNMP page. A more detailed explanation of each parameter is given below.

## SNMP Read Settings




***SNMP Versions***

| Setting | Description | Factory Default |
|---|---|---|
| Disable<br>V1, V2c, V3, or<br>V1, V2c, or<br>V3 only | Select the SNMP protocol version used to manage the secure router. | Disable |

***Contact Person***

| Setting | Description | Factory Default |
|---|---|---|
| Admin or<br>user | Admin privilege allows access and authorization to read and write the MIB file. User privilege only allows reading the MIB file, but does give authorization to write. | Admin |

***Auth. Type***

| Setting | Description | Factory Default |
|---|---|---|
| MD5 | Provides authentication based on the HMAC-MD5 algorithms. 8-character passwords are the minimum requirement for authentication. | MD5 |
| SHA | Provides authentication based on the HMAC-SHA algorithms. 8-character passwords are the minimum requirement for authentication. | |

***Data Encryption Key***

| Setting | Description | Factory Default |
|---|---|---|
| Max. 30 Characters | 8-character data encryption key is the minimum requirement for data encryption | None |

***Community Name 1/2***

| Setting | Description | Factory Default |
|---|---|---|
| Max. 30 Characters | Use a community string match for authentication | Public |

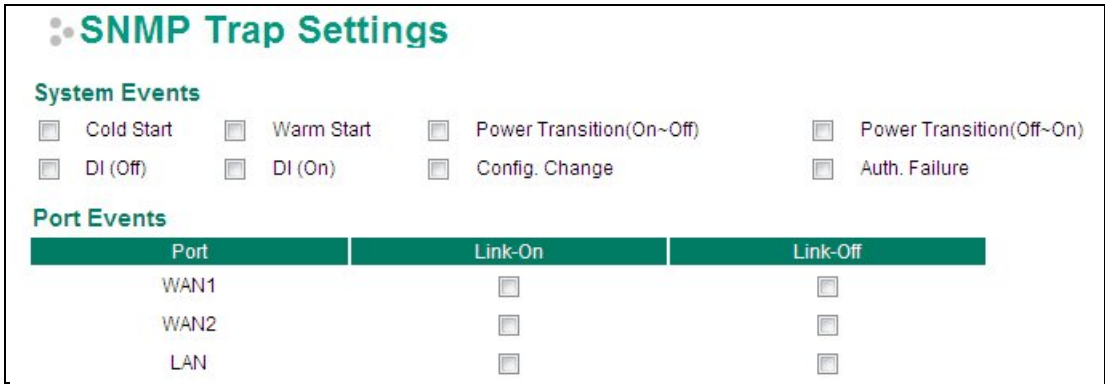
***Access Control***

| Setting | Description | Factory Default |
|---|---|---|
| Read only (Public MIB only) | Access control type after matching the community string | Read only |
| No Access | | |

***Target IP Address***

| Setting | Description | Factory Default |
|---|---|---|
| IP Address | Enter the IP address of the Trap Server used by your network. | Read only |

### SNMP Trap Type




SNMP Trap Types can be divided into two basic groups: **System Events** and **Port Events**. System Events are related to the overall function of the router, whereas Port Events are related to the activity of a specific port.

| System Events | SNMP Trap is sent when… |
|---|---|
| Cold Start | Power is cut off and then reconnected. |
| Warm Start | The Industrial Secure Router is rebooted, such as when network parameters are changed (IP address, subnet mask, etc.). |
| Power Transition (On-Off) | The Industrial Secure Router is powered down. |
| Power Transition (Off-On) | The Industrial Secure Router is powered up. |
| DI (Off) | Digital Input is triggered by an on to off transition |
| DI (On) | Digital Input is triggered by an off to on transition |
| Config. Change | A configuration item has been changed. |
| Auth. Failure | An incorrect password is entered. |

| Port Events | SNMP Trap is sent when… |
|---|---|
| Link-ON | The port is connected to another device. |
| Link-OFF | The port is disconnected (e.g., the cable is pulled out or the opposing device shuts down). |

# Using Auto Warning

Since industrial Ethernet devices are often located at the endpoints of a system, these devices will not always know what is happening elsewhere on the network. This means that an industrial Ethernet router that connects to these devices must provide system maintainers with real-time alarm messages. Even when control engineers are out of the control room for an extended period of time, they can still be informed of the status of devices almost instantaneously when exceptions occur. The Industrial Secure Router supports different approaches to warn engineers automatically, such as by using email and relay output. It also supports one digital input to integrate sensors with your system and automate alarms using email and relay output.

# Configuring Email Warning

The Auto Email Warning function uses e-mail to alert the user when certain user-configured events take place. Three basic steps are required to set up the Auto Warning function:

**1. Configure Email Event Types**

Select the desired Event types from the Web Browser **Event type** page (a description of each event type is given later in the Email Alarm Events setting subsection).

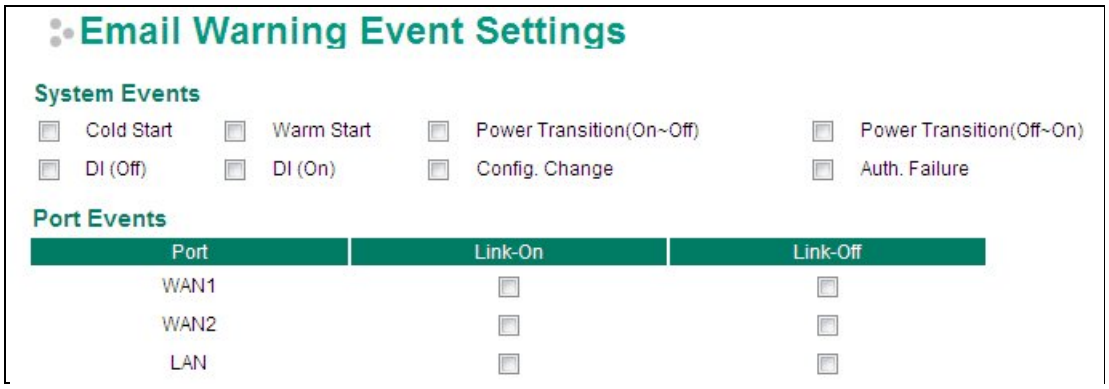
**2. Configure Email Settings**

To configure the Industrial Secure Router's email setup from a browser interface, enter your Mail Server's IP/Name (IP address or name), Account Name, Account Password, the sender's email address, and the email address to which warning messages will be sent.

**3. Activate your settings and if necessary, test the email**

After configuring and activating your Industrial Secure Router's Event Types and Email Setup, you can use the Test Email function to see if your e-mail addresses and mail server address have been properly configured.

# Event Type

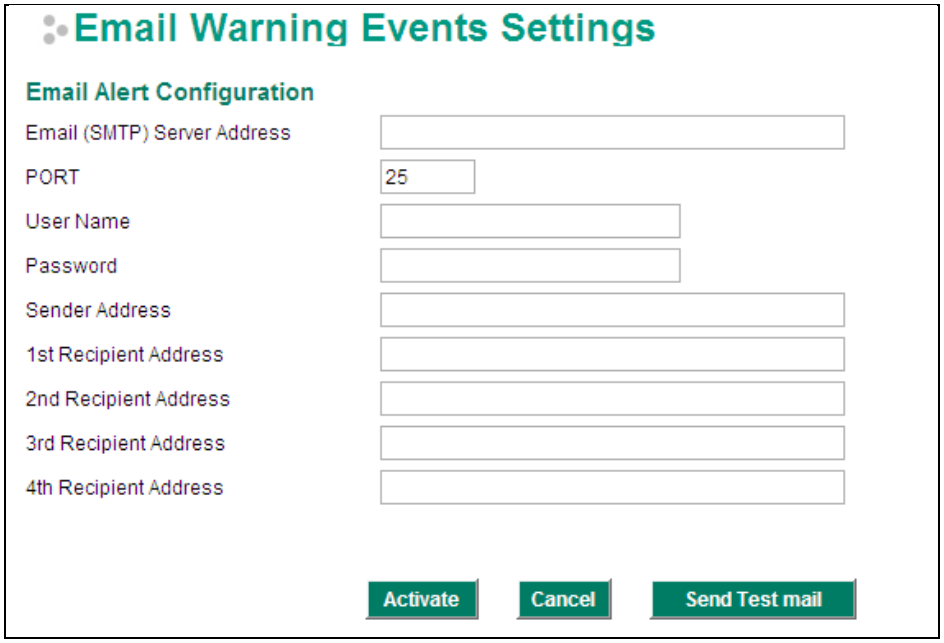



Email Warning Event Types can be divided into two basic groups: **System Events** and **Port Events**. System Events are related to the overall function of the router, whereas Port Events are related to the activity of a specific port.

| System Events | Warning email is sent when… |
|---|---|
| Cold Start | Power is cut off and then reconnected. |
| Warm Start | The Industrial Secure Router is rebooted, such as when network parameters are changed (IP address, subnet mask, etc.). |
| Power Transition (On-Off) | The Industrial Secure Router is powered down. |
| Power Transition (Off-On) | The Industrial Secure Router is powered up. |
| DI (Off) | Digital Input is triggered by on to off transition |
| DI (On) | Digital Input is triggered by off to on transition |
| Config. Change | A configuration item has been changed. |
| Auth. Failure | An incorrect password is entered. |

| Port Events | Warning email is sent when… |
|---|---|
| Link-ON | The port is connected to another device. |
| Link-OFF | The port is disconnected (e.g., the cable is pulled out or the opposing device shuts down). |

# E-mail Setup




***Main Server IP/Name***

| Setting | Description | Factory Default |
|---|---|---|
| IP address | The IP Address of your email server. | None |

***Port***

| Setting | Description | Factory Default |
|---|---|---|
| Port number | The port number of your email server. | None |

***Account Name***

| Setting | Description | Factory Default |
|---|---|---|
| Max. 30 Characters | Your email account name (typically your user name) | None |

***Email Password***

| Setting | Description | Factory Default |
|---|---|---|
| Max. 30 characters | The Password of your email account | None |

***Sender Email Address***

| Setting | Description | Factory Default |
|---|---|---|
| IP address | The IP Address of the email sender | None |

***Recipient Email Address***

| Setting | Description | Factory Default |
|---|---|---|
| Max. 50 characters | You can set up to 4 email addresses to receive alarm emails from the Industrial Secure Router. | None |

***Send Test Email***

After configuring the email settings, you should first click Activate to activate those settings, and then click **Send Test Email** to verify that the settings are correct.

**NOTE** Auto warning e-mail messages will be sent through an authentication protected SMTP server that supports the CRAM-MD5, LOGIN, and PLAIN methods of SASL (Simple Authentication and Security Layer) authentication mechanism. We strongly recommend not entering your Account Name and Account Password if auto warning e-mail messages can be delivered without using an authentication mechanism.

# Configuring Relay Warning

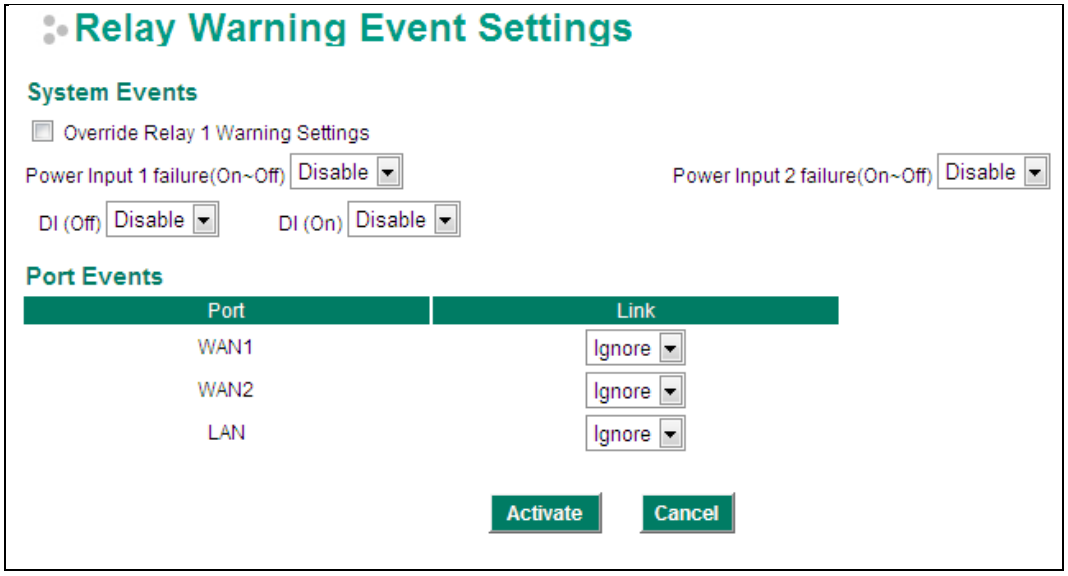
The Auto Relay Warning function uses relay output to alert the user when certain user-configured events take place. There are two basic steps required to set up the Relay Warning function:

**1. Configuring Relay Event Types**

Select the desired **Event types** from the Web Browser Event type page (a description of each event type is given later in the Relay Alarm Events setting subsection).

**2. Activate your settings**

After completing the configuration procedure, you will need to activate your Industrial Secure Router's Relay Event Types.




Event Types can be divided into two basic groups: **System Events** and **Port Events**. System Events are related to the overall function of the router, whereas Port Events are related to the activity of a specific port.

| System Events | Warning Relay output is triggered when… |
|---|---|
| Power Input 1 failure (On→Off) | Power input 1 is down. |
| Power Input 2 failure (On→Off) | Power input 2 is down. |
| DI (Off) | Digital Input is triggered by on to off transition |
| DI (On) | Digital Input is triggered by off to on transition |

| Port Events | Warning Relay output is triggered when… |
|---|---|
| Link-ON | The port is connected to another device. |
| Link-OFF | The port is disconnected (e.g., the cable is pulled out or the opposing device shuts down). |
| Ignore | Ignore the status of the port |

## Override relay warning settings

Select this option to override the relay warning setting temporarily. Releasing the relay output will allow administrators to fix any problems with the warning condition.

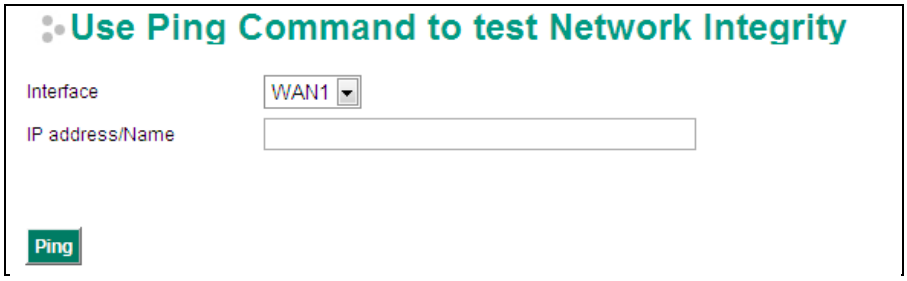
## Warning List

Use this table to see if any relay alarms have been issued.

# Using Diagnosis

The Industrial Secure Router provides **Ping** tools and **LLDP** for administrators to diagnose network systems.

## Ping

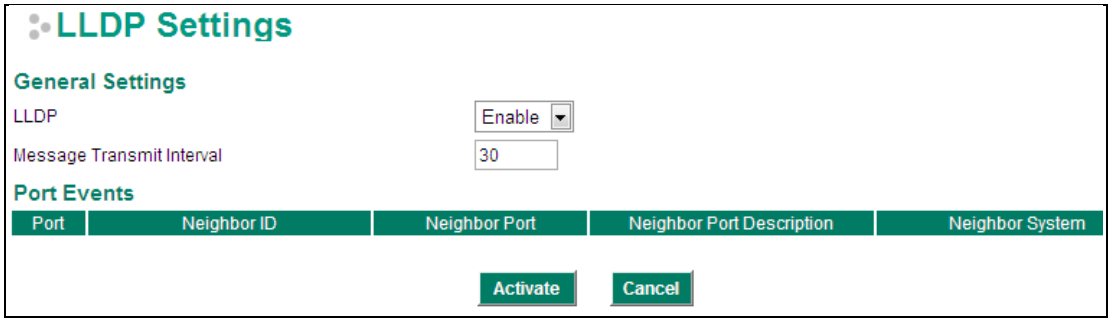



The Ping function uses the ping command to give users a simple but powerful tool for troubleshooting network problems. The function's most unique feature is that even though the ping command is entered from the user's PC keyboard, the actual ping command originates from the Industrial Secure Router itself. In this way, the user can essentially control the Industrial Secure Router and send ping commands out through its ports. There are two basic steps required to set up the Ping command to test network integrity:

1. Select which interface will be used to send the ping commands. You may choose from WAN1, WAN2, and LAN.
2. Type in the desired IP address, and click Ping.

## LLDP Function Overview

Defined by IEEE 802.11AB, Link Layer Discovery Protocol (LLDP) is an OSI Layer 2 Protocol that standardizes the methodology of self-identity advertisement. It allows each networking device, such as a Moxa managed switch/router, to periodically inform its neighbors about itself and its configuration. In this way, all devices will be aware of each other.




The router's web interface can be used to enable or disable LLDP, and to set the LLDP **Message Transmit Interval**. Users can view each switch's neighbor-list, which is reported by its network neighbors.

## LLDP Setting

***Enable LLDP***

| Setting | Description | Factory Default |
|---|---|---|
| Enable or Disable | Enable or disable LLDP function. | Enable |

***Message Transmit Interval***

| Setting | Description | Factory Default |
|---|---|---|
| 5 to 32768 sec. | Set the transmit interval of LLDP messages. Unit is in seconds. | 30 (sec.) |

## LLDT Table

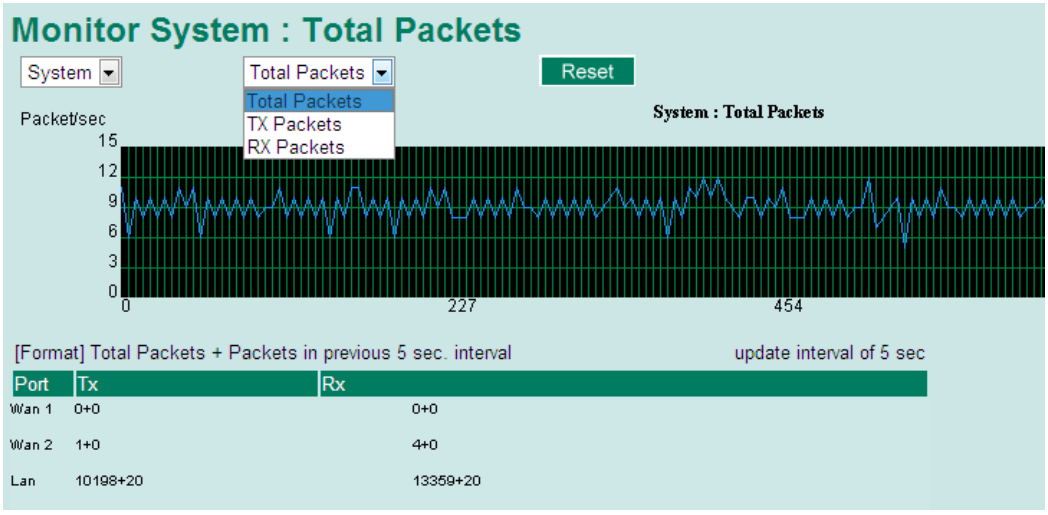
**Port:** The port number that connects to the neighbor device.
**Neighbor ID:** A unique entity that identifies a neighbor device; this is typically the MAC address.
**Neighbor Port:** The port number of the neighbor device.
**Neighbor Port Description:** A textual description of the neighbor device's interface.
**Neighbor System:** Hostname of the neighbor device.

# Using Monitor

You can monitor statistics in real time from the Industrial Secure Router's web console.

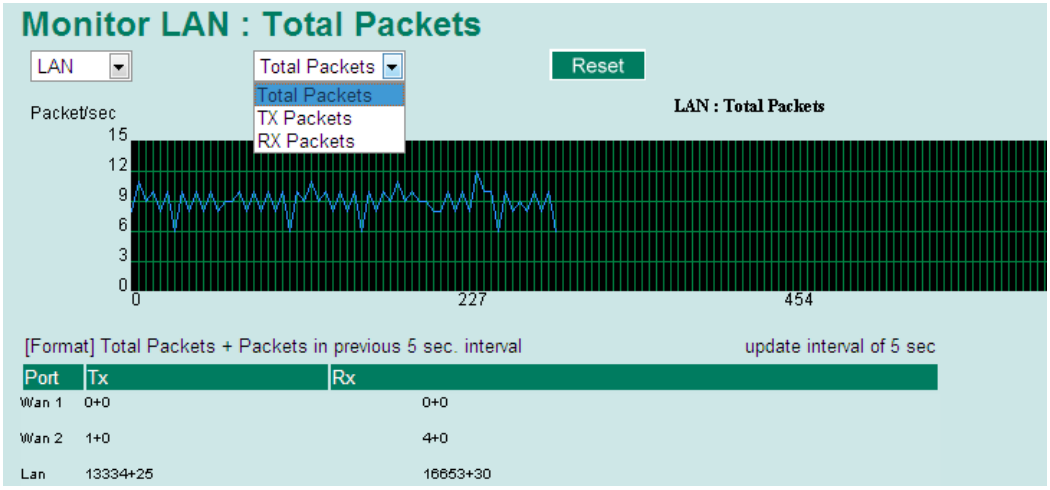
## Monitor by System

Access the Monitor by selecting "System" from the left selection bar. Monitor by System allows the user to view a graph that shows the combined data transmission activity of all the Industrial Secure Router's 3 ports. Click one of the three options—Total Packets, TX Packets or RX Packets—to view transmission activity of specific types of packets. Recall that TX Packets are packets sent out from the Industrial Secure Router, and RX Packets are packets received from connected devices. The Total Packets option displays a graph that combines TX and RX activity. The graph displays data transmission activity by showing **Packets/s** (i.e., packets per second, or pps) versus **sec.** (seconds).The graph is updated every few seconds, allowing you to analyze data transmission activity in real time.




## Monitor by Port

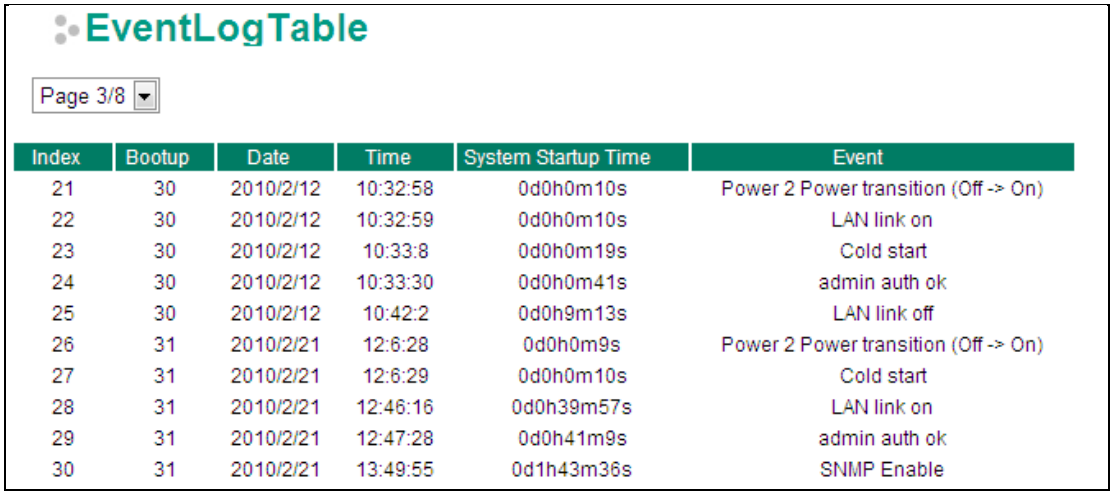
Access the Monitor by Port function by selecting the WAN1, WAN2, or LAN interface from the left drop-down list. You can view graphs that show All Packets, TX Packets, or RX Packets, but in this case, only for an individual port. The graph displays data transmission activity by showing **Packets/s** (i.e., packets per second, or pps) versus **sec.** (seconds).The graph is updated every few seconds, allowing you to analyze data transmission activity in real time.



# Using System Log

The Industrial Secure Router provides **EventLog** and **Syslog** functions to record important events.

## Using EventLog


EventLogTable

Page 3/8

| Index | Bootup | Date | Time | System Startup Time | Event |
|---|---|---|---|---|---|
| 21 | 30 | 2010/2/12 | 10:32:58 | 0d0h0m10s | Power 2 Power transition (Off -> On) |
| 22 | 30 | 2010/2/12 | 10:32:59 | 0d0h0m10s | LAN link on |
| 23 | 30 | 2010/2/12 | 10:33:8 | 0d0h0m19s | Cold start |
| 24 | 30 | 2010/2/12 | 10:33:30 | 0d0h0m41s | admin auth ok |
| 25 | 30 | 2010/2/12 | 10:42:2 | 0d0h9m13s | LAN link off |
| 26 | 31 | 2010/2/21 | 12:6:28 | 0d0h0m9s | Power 2 Power transition (Off -> On) |
| 27 | 31 | 2010/2/21 | 12:6:29 | 0d0h0m10s | Cold start |
| 28 | 31 | 2010/2/21 | 12:46:16 | 0d0h39m57s | LAN link on |
| 29 | 31 | 2010/2/21 | 12:47:28 | 0d0h41m9s | admin auth ok |
| 30 | 31 | 2010/2/21 | 13:49:55 | 0d1h43m36s | SNMP Enable |

| Field | Description |
|---|---|
| Bootup | This field shows how many times the EDR-G509 has been rebooted or cold started. |
| Date | The date is updated based on how the current date is set in the "Basic Setting" page. |
| Time | The time is updated based on how the current time is set in the "Basic Setting" page. |
| System Startup Time | The system startup time related to this event. |
| Event | Events that have occurred. |

The following events will be recorded in the Industrial Secure Router EventLog Table:

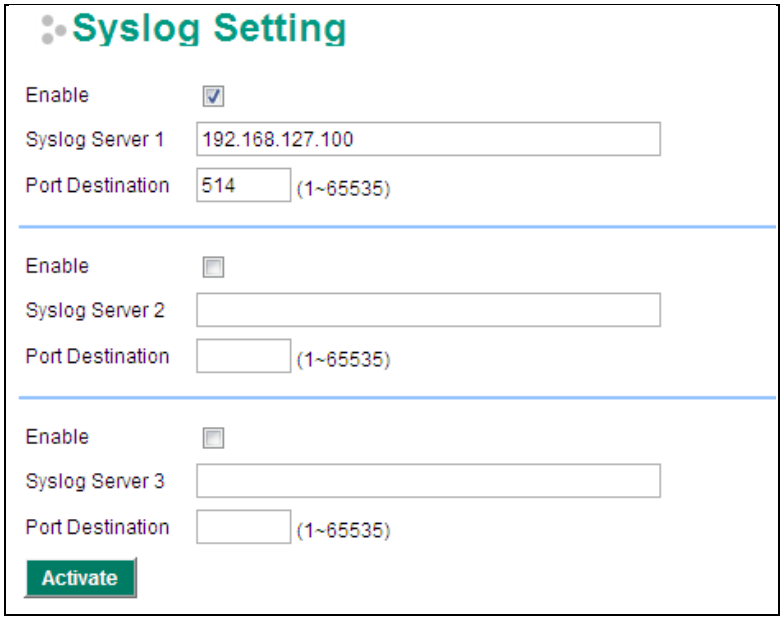
| Event | Status |
|---|---|
| Syslog | Configuration change activated |
| DNS | Configuration change activated |
| Static Route | Configuration change activated |
| SYSTEMINFO | Configuration change activated |
| SNMPTRAP | Configuration change activated |
| Filter | Configuration change activated |
| NAT | Configuration change activated |
| DoS | Configuration change activated |
| QoS_Bandwith | Configuration change activated |
| QoS_DownStream | Configuration change activated |
| QoS_UpStream | Configuration change activated |
| DHCP | Configuration Change activated/ Enable / Disable |
| NTP | Configuration Change activated/ Enable / Disable |
| SNMP | Configuration Change activated/ Enable / Disable |
| DDNS | Configuration Change activated/ Enable / Disable |
| WAN Backup | Configuration change activated |
| LAN | Link on / Link off / IP change |
| WAN2 | Link on / Link off / IP change |
| WAN1 | Link on / Link off / IP change |
| Password | Configuration change activated |
| Login | Authentication Fail / Authentication Pass |
| Accessible IP function | Enable / Disable |
| Power transition (On -> Off) | |
| Power transition (Off -> On) | |

| | |
|---|---|
| DI transition (Off -> On) | |
| DI transition (On -> Off) | |
| Cold start | |
| Factory default | Warm start |
| System restart | Warm start |
| Firmware Upgrade | Warm start |
| Configuration Upgrade | Warm start |

**NOTE** The maximum number of event entries is 1000.

# Using Syslog

This function provides the event logs for the syslog server. The function supports 3 configurable syslog servers and syslog server UDP port numbers. When an event occurs, the event will be sent as a syslog UDP packet to the specified syslog servers.




***Syslog Server 1/2/3***

| Setting | Description | Factory Default |
|---|---|---|
| IP Address | Enter the IP address of the Syslog Server used by your network. | None |
| Port Destination (1 to 65535) | Enter the UDP port of the Syslog Server. | 514 |

# Using HTTPs/SSL

To secure your HTTP access, the Industrial Secure Router supports HTTPS/SSL to encrypt all HTTP traffic. Perform the following steps to access the Industrial Secure Router's web browser interface via HTTPS/SSL.

1. Open Internet Explorer and type https://< Industrial Secure Router's IP address> in the address field. Press Enter to establish the connection.

2. A warning message will appear to warn the user that the security certificate was issued by a company they have not chosen to trust.

Security Alert
Information you exchange with this site cannot be viewed or changed by others. However, there is a problem with the site's security certificate.
The security certificate was issued by a company you have not chosen to trust. View the certificate to determine whether you want to trust the certifying authority.
The security certificate date is valid.
The name on the security certificate is invalid or does not match the name of the site
Do you want to proceed?
Yes
No
View Certificate

3. Select **Yes** to enter the Industrial Secure Router's web browser interface and access the web browser interface secured via HTTPS/SSL.

# A

# MIB Groups

The Industrial Secure Router comes with built-in SNMP (Simple Network Management Protocol) agent software that supports cold start trap, line up/down trap, and RFC 1213 MIB-II. The standard MIB groups that the Industrial Secure Router series support are:

**MIB II.1 – System Group**

sysORTable

**MIB II.2 – Interfaces Group**

ifTable

**MIB II.4 – IP Group**

ipAddrTable
ipNetToMediaTable
IpGroup
IpBasicStatsGroup
IpStatsGroup

**MIB II.5 – ICMP Group**

IcmpGroup
IcmpInputStatus
IcmpOutputStats

**MIB II.6 – TCP Group**

tcpConnTable
TcpGroup
TcpStats

**MIB II.7 – UDP Group**

udpTable
UdpStats

**MIB II.11 – SNMP Group**

SnmpBasicGroup
SnmpInputStats
SnmpOutputStats

**Public Traps**

1. Cold Start
2. Link Up
3. Link Down
4. Authentication Failure

**Private Traps:**

1. Configuration Changed
2. Power On
3. Power Off
4. DI Trap

The Industrial Secure Router also provides a MIB file, located in the file "Moxa-EDRG903-MIB.my" on the Industrial Secure Router Series utility CD-ROM for SNMP trap message interpretation